UNCLASSIFIED

Symantec AntiVirus Managed Client

Version: 4

Release: 1

03 Dec 2009

STIG.DOD.MIL

Sort Order: Group ID (Vulid), ascending order
Notice: Developed by DISA for the DoD
Description:

CIRCLE ONE

FOR OFFICIAL USE ONLY (mark each page)

CONFIDENTIAL and SECRET (mark each page and each finding)

Classification is based on classification of system reviewed:

Unclassified System = FOUO Checklist
Confidential System = CONFIDENTIAL Checklist
Secret System= SECRET Checklist
Top Secret System = SECRET Checklist

Group ID (Vulid): V-6359
Group Title: DTAS002-Symantec Antivirus not configured to resta
Rule ID: SV-21120r1_rule
Severity: CAT II
Rule Version (STIG-ID): DTAS002
Rule Title: The Symantec Antivirus is not configured to restart for configuration changes.

Vulnerability Discussion: Without an automatic restart, changes to the virus protection will not be in effect until a reboot of the machine.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\ INTEL\LANDesk\VirusProtect6\CurrentVersion\
Storages\Filesystem\RealTimeScan
Criteria: If the value of ConfigRestart is 1, this is not a finding.

Check Content:
Server check: From the Symantec Enterprise Server, Symantec System Center Console: select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Client Auto-Protect Options -> File System tab -> Advanced -> Ensure “Stop and reload Auto-Protect” is selected.

Criteria: If the option “Stop and reload Auto-Protect” is selected, this is not a finding.

Fix Text: From the Symantec Enterprise Server, Symantec System Center Console: select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Client Auto-Protect Options -> File System tab -> Advanced -> In the Changes requiring Auto-protect reload area, select “Stop and reload Auto-Protect”.

Group ID (Vulid): V-6360
Group Title: DTAS003-Symantec Antivirus autoprotect
Rule ID: SV-23671r1_rule
Severity: CAT I
Rule Version (STIG-ID): DTAS003
Rule Title: The Symantec Antivirus autoprotect parameter is incorrect.

Vulnerability Discussion: Without autoprotect, the virus scan is not scanning files as they are being accessed.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\ INTEL\LANDesk\VirusProtect6\CurrentVersion\
Storages\Filesystem\RealTimeScan
Criteria: If the value of OnOff is 1, this is not a finding.

Check Content:
From the Symantec Enterprise Server, Symantec System Center Console: select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Client Auto-Protect Options -> File System tab -> Ensure “Enable Auto-Protect” is selected.

Criteria: If the option “Enable Auto-Protect” is selected, this is not a finding.

Fix Text: From the Symantec Enterprise Server, Symantec System Center Console: select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Client Auto-Protect Options -> File System tab -> select “Enable Auto-Protect”.

Group ID (Vulid): V-6361
Group Title: DTAS004-Symantec Antivirus auto protect-All Files
Rule ID: SV-21118r1_rule
Severity: CAT II
Rule Version (STIG-ID): DTAS004
Rule Title: The Symantec Antivirus auto protect-All Files configuration is incorrect.

Vulnerability Discussion: All files must be included in virus scans for the scans to be effective.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\ INTEL\LANDesk\VirusProtect6\CurrentVersion\
Storages\Filesystem\RealTimeScan
Criteria: If the value of FileType is 0, this is not a finding.

Check Content:
From the Symantec Enterprise Server, Symantec System Center Console: select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Client Auto-Protect Options -> File System tab -> Ensure the option “All Types” is selected.

Criteria: If the option “All Types” is selected, this is not a finding.

Fix Text: From the Symantec Enterprise Server, Symantec System Center Console: select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Client Auto-Protect Options -> File System tab -> in the File Types area, select “All Types”.

Group ID (Vulid): V-6362
Group Title: DTAS006-Symantec Antivirus display message
Rule ID: SV-21117r1_rule
Severity: CAT II
Rule Version (STIG-ID): DTAS006

Rule Title: The Symantec Antivirus display message parameter is incorrect.

Vulnerability Discussion: Without an appropriate message when an infection is found, the user will not know there is a virus.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\ INTEL\LANDesk\VirusProtect6\CurrentVersion\
Storages\Filesystem\RealTimeScan
Criteria: If the value of MessageBox is 1, this is not a finding.

Check Content:
From the Symantec Enterprise Server, Symantec System Center Console: select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Client Auto-Protect Options -> File System tab -> Notifications -> Detections Options -> Ensure “Display notification message on infected computer” is selected.

Criteria: If the option “Display notification message on infected computer” is selected, this is not a finding.

Fix Text: From the Symantec Enterprise Server, Symantec System Center Console: select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Client Auto-Protect Options -> File System tab -> Notifications -> Detections Options -> Select “Display notification message on infected computer”.

Group ID (Vulid): V-6363
Group Title: DTAS007-Symantec Antivirus exclude files configura
Rule ID: SV-21116r1_rule
Severity: CAT II
Rule Version (STIG-ID): DTAS007
Rule Title: The Symantec Antivirus exclude files configuration is incorrect.

Vulnerability Discussion: The “Exclude selected files and folders” is used to exclude files and folders from a scan. This requirement maintains that no files or folders are excluded from the scan by ensuring that this attribute is not selected.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\ INTEL\LANDesk\VirusProtect6\CurrentVersion\
Storages\Filesystem\RealTimeScan
Criteria: If the value of ExcludedByExtensions is 0, this is not a finding.

Check Content:
From the Symantec Enterprise Server, Symantec System Center Console: select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Client Auto-Protect Options -> File System tab -> Ensure that “Exclude selected files and folders” is not selected.

Criteria: If the option “Exclude selected files and folders” is not selected, this is not a finding.

Note: Network drives and folders may be excluded from local scans. Evaluate exclusions with SA.

Fix Text: From the Symantec Enterprise Server, Symantec System Center Console: select System Hierarchy ->

select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Client Auto-Protect Options -> File System tab -> In the Options area, de-select “Exclude selected files and folders”.

Group ID (Vulid): V-6368
Group Title: DTAS012-Symantec Antivirus autoprotect read
Rule ID: SV-21121r1_rule
Severity: CAT II
Rule Version (STIG-ID): DTAS012
Rule Title: The Symantec Antivirus autoprotect read parameter is incorrect.

Vulnerability Discussion: Without this parameter, files that are accessed by the user will not be checked for viruses.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\ INTEL\LANDesk\VirusProtect6\CurrentVersion\
Storages\Filesystem\RealTimeScan
Criteria: If the value of Reads is 1, this is not a finding.

Check Content:
From the Symantec Enterprise Server, Symantec System Center Console: select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Client Auto-Protect Options -> File System tab -> Advanced -> Ensure “Accessed or modified (scan on create, open, move, copy, or run), is selected.

Criteria: If the option “Accessed or modified (scan on create, open, move, copy, or run)” is selected, this is not a finding.

Fix Text: From the Symantec Enterprise Server, Symantec System Center Console: select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Client Auto-Protect Options -> File System tab -> Advanced -> In the Scan files when area, select “Accessed or modified (scan on create, open, move, copy, or run)".

Group ID (Vulid): V-6369
Group Title: DTAS013-Symantec Antivirus AutoProtect backup opti
Rule ID: SV-21122r1_rule
Severity: CAT II
Rule Version (STIG-ID): DTAS013
Rule Title: The Symantec Antivirus AutoProtect parameter for backup options is incorrect.

Vulnerability Discussion: Without setting this parameter, a copy of the file will not be saved before trying to remove the virus.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\ INTEL\LANDesk\VirusProtect6\CurrentVersion\
Storages\Filesystem\RealTimeScan

Criteria: If the value of BackupToQuarantine is 1, this is not a finding.

Check Content:
From the Symantec Enterprise Server, Symantec System Center Console: select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> File System tab -> Client Auto-Protect Options -> Advanced -> select “Back up file before attempting to repair”.

Criteria: If the option “Back up file before attempting to repair” is selected, this is not a finding.

Fix Text: From the Symantec Enterprise Server, Symantec System Center Console: select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Client Auto-Protect Options -> File System tab -> Advanced -> In the Backup Options area, select “Back up file before attempting to repair”.

Group ID (Vulid): V-6370
Group Title: DTAS014-Symantec Antivirus AutoProtect autoenabler
Rule ID: SV-21143r1_rule
Severity: CAT II
Rule Version (STIG-ID): DTAS014
Rule Title: The Symantec Antivirus AutoProtect parameter for autoenabler is incorrect.

Vulnerability Discussion: If virus checking is turned off, this parameter will turn it back on after 5 minutes. This will ensure the virus checking program will remain on even if the user turns it off.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\ INTEL\LANDesk\VirusProtect6\CurrentVersion\
Storages\Filesystem\RealTimeScan

Criteria: If the value of APEOn is 1 and the value of APESleep is <=5 , this is not a finding. If APESleep is > 5 or APEOn is not 1, this is a finding.

Check Content:
From the Symantec Enterprise Server, Symantec System Center Console: select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Client Auto-Protect Options -> File System tab -> Advanced -> In the Automatic enabler area, select “When Auto-Protect is disabled, enable after:”. Additionally, select minutes must be <= 5.

Criteria: If the option “When Auto-Protect is disabled, enable after:” is selected and selected minutes is <= 5, this is not a finding.

Fix Text: From the Symantec Enterprise Server, Symantec System Center Console: select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Client Auto-Protect Options -> File System tab -> Advanced -> In the Automatic enabler area, select “When Auto-Protect is disabled, enable after:”. Additionally, select minutes must be <= 5.

Group ID (Vulid): V-6371

Group Title: DTAS015-Symantec Antivirus AutoProtect floppies
Rule ID: SV-21123r1_rule
Severity: CAT II
Rule Version (STIG-ID): DTAS015
Rule Title: The Symantec Antivirus AutoProtect parameter for floppies is incorrect.

Vulnerability Discussion: This parameter determines whether floppy disk are checked for viruses.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\ INTEL\LANDesk\VirusProtect6\CurrentVersion\Storages\Filesystem\RealTimeScan
Criteria: If the value of ScanFloppyBRonAccess is 1, this is not a finding.

Check Content:
From the Symantec Enterprise Server, Symantec System Center Console: select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Client Auto-Protect Options -> File System tab -> Advanced -> Floppies -> Ensure “Check floppies for boot viruses upon access” is selected.

Criteria: If the option “Check floppies for boot viruses upon access” is selected, this is not a finding.

Fix Text: From the Symantec Enterprise Server, Symantec System Center Console: select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Client Auto-Protect Options -> File System tab -> Advanced -> Floppies -> In the Floppy settings area, select “Check floppies for boot viruses upon access”.

Group ID (Vulid): V-6372
Group Title: DTAS016-Symantec Antivirus AutoProtect Boot virus
Rule ID: SV-21124r1_rule
Severity: CAT II
Rule Version (STIG-ID): DTAS016
Rule Title: The Symantec Antivirus AutoProtect parameter for Boot virus is incorrect.

Vulnerability Discussion: This parameter tells the antivirus program what to do when a boot virus is found.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\ INTEL\LANDesk\VirusProtect6\CurrentVersion\
Storages\Filesystem\RealTimeScan
Criteria: If the value of FloppyBRAction is 5, this is not a finding.

Check Content:
From the Symantec Enterprise Server, Symantec System Center Console: select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Client Auto-Protect Options -> File System tab -> Advanced -> Floppies -> In the Floppy settings area under the When a boot virus is found pull down menu, ensure that “Clean virus from boot record” is selected.

Criteria: If the option “Clean virus from boot record” is selected, this is not a finding.

Fix Text: From the Symantec Enterprise Server, Symantec System Center Console: select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec

Antivirus -> Client Auto-Protect Options -> File System tab -> Advanced -> Floppies -> In the Floppy settings area; select in the When a boot virus is found pull down menu, select “Clean virus from boot record”.

Group ID (Vulid): V-6374
Group Title: DTAS017-Symantec Antivirus AutoProtect floppy shut
Rule ID: SV-21125r1_rule
Severity: CAT II
Rule Version (STIG-ID): DTAS017
Rule Title: The Symantec Antivirus AutoProtect parameter for check floppy at shutdown is incorrect.

Vulnerability Discussion: This checks floppy drives at shutdown time.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\ INTEL\LANDesk\VirusProtect6\CurrentVersion\
Storages\Filesystem\RealTimeScan
Criteria:
For Version 9.x If the value of SkipFloppyBRonAccess is 0, this is not a finding.
For Version 10.x If the value of SkipShutDownFloppyCheck is 0x0, this is not a finding.

Check Content:
From the Symantec Enterprise Server, Symantec System Center Console: select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Client Auto-Protect Options -> File System tab -> Advanced -> Floppies -> Ensure “Do not check floppies upon system shutdown” is not selected.

Criteria: If the option “Do not check floppies upon system shutdown” is not selected, this is not a finding.

Fix Text: From the Symantec Enterprise Server, Symantec System Center Console: select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Client Auto-Protect Options -> File System tab -> Advanced -> Floppies -> In the Floppy settings area, de-select (uncheck) “Do not check floppies upon system shutdown”.

Group ID (Vulid): V-6375
Group Title: DTAS020-Symantec Antivirus email for Boot sectors
Rule ID: SV-21126r1_rule
Severity: CAT II
Rule Version (STIG-ID): DTAS020
Rule Title: The Symantec Antivirus email parameter for Boot sectors is incorrect.

Vulnerability Discussion: This parameter controls whether or not email is scanned.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\ INTEL\LANDesk\VirusProtect6\CurrentVersion\
Storages\EmailName\RealTimeScan
Criteria: If the value of OnOff is 1, this is not a finding.
Note: This check is for email clients. Substitute your email application name (InternetMail,

LotusNotes, or MicrosoftExchangeClient) into the registry string indicated by EmailName.
If email client is not installed, this check is NA.

Check Content:
From the Symantec Enterprise Server, Symantec System Center Console: select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Client Auto-Protect Options -> email name tab (where “email name” is the email client type; options are Internet E-mail, Lotus Notes, and Microsoft Exchange) -> Ensure “Enable “email name” Auto-Protect” is selected.

Criteria: If the option “Enable “email name” Auto-Protect” is selected, this is not a finding.

Fix Text: From the Symantec Enterprise Server, Symantec System Center Console: select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Client Auto-Protect Options -> email name tab (where “email name” is the email client type; options are Internet E-mail, Lotus Notes, or Microsoft Exchange) -> select “Enable “email name” Auto-Protect”.

Group ID (Vulid): V-6376
Group Title: DTAS021-Symantec Antivirus email client for files
Rule ID: SV-21128r1_rule
Severity: CAT II
Rule Version (STIG-ID): DTAS021
Rule Title: The Symantec Antivirus email client parameter for all files is incorrect.

Vulnerability Discussion: This controls whether or not files are checked for viruses.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\ INTEL\LANDesk\VirusProtect6\CurrentVersion\
Storages\EmailName\RealTimeScan
Criteria: If the value of FileType is 0, this is not a finding.
Note: This check is for email clients. Substitute your email application name (InternetMail, LotusNotes, or MicrosoftExchangeClient) into the registry string indicated by EmailName.
If email client is not installed, this check is NA.

Check Content:
From the Symantec Enterprise Server, Symantec System Center Console: select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Client Auto-Protect Options -> email name tab (where “email name” is the email client type; options are Internet E-mail, Lotus Notes, and Microsoft Exchange) -> Ensure “All types” is selected.

Criteria: If the option “All types” is selected, this is not a finding.

Fix Text: From the Symantec Enterprise Server, Symantec System Center Console: select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Client Auto-Protect Options -> email name tab (where “email name” is the email client type; options are Internet E-mail, Lotus Notes, or Microsoft Exchange) -> In the File Types area, select “All types”.

Group ID (Vulid): V-6383
Group Title: DTAS029-Symantec Antivirus email client compressed

Rule ID: SV-21130r1_rule
Severity: CAT II
Rule Version (STIG-ID): DTAS029
Rule Title: The Symantec Antivirus email client parameter for compressed files is incorrect.

Vulnerability Discussion: This controls what happens when the program encounters compressed files.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\ INTEL\LANDesk\VirusProtect6\CurrentVersion\
Storages\EmailName\RealTimeScan
Criteria: If the value of ZipFile is 1, this is not a finding.
Note: This check is for email clients. Substitute your email application name (InternetMail, LotusNotes, or MicrosoftExchangeClient) into the registry string indicated by EmailName.
If email client is not installed, this check is NA.

Check Content:
From the Symantec Enterprise Server, Symantec System Center Console: select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Client Auto-Protect Options -> email name tab (where “email name” is the email client type; options are Internet E-mail, Lotus Notes, and Microsoft Exchange) -> Advanced -> Ensure “Scan files inside compressed files” is selected.

Criteria: If the option “Scan files inside compressed files” is selected, this is not a finding.

Fix Text: From the Symantec Enterprise Server, Symantec System Center Console: select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Client Auto-Protect Options -> email name tab (where “email name” is the email client type; options are Internet E-mail, Lotus Notes, or Microsoft Exchange) -> Advanced ->In the When scanning inside compressed files area, select “Scan files inside compressed files”.

Group ID (Vulid): V-6384
Group Title: DTAS030-Symantec AntiVirus CE History Options
Rule ID: SV-23672r1_rule
Severity: CAT II
Rule Version (STIG-ID): DTAS030
Rule Title: The Symantec AntiVirus CE History Options parameters are not configured as required.

Vulnerability Discussion: This parameter deteremines the log history of the antivirus program.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\INTEL\LANDesk\VirusProtect6\CurrentVersion
and determine the value data for the LogFileRollOverDays and LogFrequency values.
Criteria: If the value data for the LogFileRollOverDays values is not 1e (the hex value for 30) or higher, this is a Finding.
If the value data for the LogFrequency value is not 0 (the number zero), this is a Finding.
Note: The LogFileRollOverDays and LogFrequency values are not created through a default product installation. The absence of these values is considered a Finding, because it allows the

vendor default to be used and that value could be changed through vendor maintenance.

Check Content:
From the Symantec Enterprise Server, Symantec System Center Console: select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Configure History ->In the History Options - Delete histories area, select “Delete after” 30 days or longer time period.

Criteria: If the option “Delete after” is greater than or equal to 30, this is not a finding.

Fix Text: From the Symantec Enterprise Server, Symantec System Center Console: select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Configure History ->In the History Options - Delete histories area, select “Delete after” 30 days or longer time period.

Group ID (Vulid): V-6385
Group Title: DTAS031-Symantec Antivirus not scheduled to autoup
Rule ID: SV-23673r1_rule
Severity: CAT II
Rule Version (STIG-ID): DTAS031
Rule Title: The Symantec Antivirus is not scheduled to autoupdate.

Vulnerability Discussion: This parameter controls the automation of updates to the signature files

Responsibility: System Administrator

Check Content:
This is a two part check.The primary server must be checked to ensure that it is being updated as required.

From the Symantec Enterprise Server- Symantec System Center Console - System Center Console on the Enterprise Server: System Hierarchy -> select (right click) Primary Server -> All Tasks -> Symantec Antivirus -> Virus Definition Manager -> Configure -> "Schedule for automatic updates" is checked -> Select Schedule: ensure the update is scheduled on at least a weekly basis.

SECOND, the client configuration must be checked.

From the System Center Console on the Enterprise Server select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Virus Definition Manager -> If "Update virus definitions from parent server" is checked, the Schedule is not necessary. If “Schedule for automated updates using LiveUpdate" is checked -> select Schedule: ensure the update is scheduled on at least a weekly basis.

Criteria: If the Schedule for Automatic Updates is defined for at least a weekly update, this is not a finding.

Fix Text: This is a two part check. FIRST, the primary server must be checked to ensure that it is being updated as required.

From the Symantec Enterprise Server- Symantec System Center Console - System Center Console on the Enterprise Server: System Hierarchy -> select (right click) Primary Server -> All Tasks -> Symantec Antivirus -> Virus Definition Manager -> Configure -> select "Schedule for automatic updates" -> select Schedule: select the update to be scheduled on at least a weekly basis.

SECOND, the client configuration must be checked.

From the System Center Console on the Enterprise Server, select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Virus Definition Manager -> If "Update virus definitions from parent server" is checked, checking the Schedule is not necessary. If “Schedule for automated updates using LiveUpdate" is checked -> select Schedule: Ensure the update is scheduled on at least a weekly basis.

Group ID (Vulid): V-6386
Group Title: DTAS032-no Symantec Antivirus Scheduled Scans
Rule ID: SV-21132r1_rule
Severity: CAT II
Rule Version (STIG-ID): DTAS032
Rule Title: There is no Symantec Antivirus Scheduled Scans or Startup Scans task configured to scan local drive(s) at least weekly.

Vulnerability Discussion: This controls the automatic scan of all local drives.

Responsibility: System Administrator

Check Content:
From the Symantec Enterprise Server, Symantec System Center Console: A determination of the existence of a weekly scan must be made. Select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Scheduled Scans -> In the Client Scans area, if there are no scans (at least weekly) defined, one must be created.

To make this determination on the client machine, navigate to the following registry key: HKLM\Software\Intel\Landesk\VirusProtect6\CurrentVersion\LocalScans. Review the ClientServerScheduledScan_1\Schedule key. This key contains a value for Type that determines the frequency of the scan. If the value for this key is a 1 or a 2, this is a daily or a weekly scan.

Note: In the key ClientServerScheduledScan_1, the 1 indicates the entry number for the scan. It may be necessary to review all ClientServerScheduledScan_X keys in the LocalScans branch to evaluate this check as each ClientServerScheduledScan_X may have a different frequency. Make note of the ClientServerScheduledScan_X weekly scan key as this will be the key used in following weekly scan checks.

Criteria: If the value of Type is 1 or 2 and the value of Enabled is 1, this is not a finding.

Fix Text: From the Symantec Enterprise Server, Symantec System Center Console: A determination of the existence of a weekly scan must be made. Select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Scheduled Scans -> In the Client Scans area, examine the entries in this list. Under the When column, the schedule for each scan can be determined. If no weekly scan exists, one must be created. Select New -> in the Name: “provide scan name” -> select Enable scan -> select Frequency of at least weekly.

Criteria: If a weekly scan exists, this is not a finding.

Group ID (Vulid): V-6387
Group Title: DTAS037-Symantec Antivirus weekly scan for files
Rule ID: SV-23675r1_rule
Severity: CAT II
Rule Version (STIG-ID): DTAS037

Rule Title: The Symantec Antivirus weekly scan parameter for all files is incorrect.

Vulnerability Discussion: This parameter ensures all files are scanned during the weekly scan.

Responsibility: System Administrator

Check Content:
From the Symantec Enterprise Server - Symantec System Center Console, review each Scheduled Scan. From the Symantec System Center Console, select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Scheduled Scans -> Highlight the client server “weekly scan” -> select Edit -> select Scan Settings -> In the File types area, ensure “All Types” is selected.

Criteria: If the option “All Types” is selected, this is not a finding.

To make this determination on the client machine, navigate to the following registry key:
HKLM\Software\Intel\Landesk\VirusProtect6\CurrentVersion\LocalScans. Review the ClientServerScheduledScan_1 key.
Note: In the key ClientServerScheduledScan_1, the 1 indicates the entry number for the scan. It may be necessary to review all ClientServerScheduledScan_X keys in the LocalScans branch to evaluate this check.

Criteria: If the value of FileType is 1, this is not a finding.

Fix Text: From the Symantec Enterprise Server- Symantec System Center Console, review each Scheduled Scan. Select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Scheduled Scans -> Highlight the client server “weekly scan” -> select Edit -> select Scan Settings -> select “All Types”.

Group ID (Vulid): V-6388
Group Title: DTAS040-Symantec Antivirus weekly scan memory
Rule ID: SV-23705r1_rule
Severity: CAT II
Rule Version (STIG-ID): DTAS040
Rule Title: The Symantec Antivirus weekly scan parameter for memory enabled is incorrect.

Vulnerability Discussion: This parameter ensures memory is scanned during the weekly scan.

Responsibility: System Administrator

Check Content:
From the Symantec Enterprise Server- Symantec System Center Console, review each Scheduled Scan. From the Enterprise Console select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Scheduled Scans -> Highlight the client server “weekly scan” -> select Edit -> select Scan Settings -> In the Scan settings area, ensure “Memory” is selected.

Criteria: If the option “Memory” is selected, this is not a finding.

To make this determination on the client machine, navigate to the following registry key:
HKLM\Software\Intel\Landesk\VirusProtect6\CurrentVersion\LocalScans\ClientServerScheduledScan_1.
Note: In the key ClientServerScheduledScan_1, the 1 indicates the entry number for the scan. It may be necessary to review all ClientServerScheduledScan_X keys in the LocalScans branch to evaluate this check.

Criteria: If the value of ScanProcess is 1, this is not a finding.

Fix Text: From the Symantec Enterprise Server- Symantec System Center Console, select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Scheduled Scans -> Highlight the client server weekly scan -> select Edit -> select Scan Settings -> select “Memory”.

Group ID (Vulid): V-6389
Group Title: DTAS041-Symantec Antivirus weekly scan messages
Rule ID: SV-21058r1_rule
Severity: CAT II
Rule Version (STIG-ID): DTAS041
Rule Title: The Symantec Antivirus weekly scan parameter for messages is incorrect.

Vulnerability Discussion: This parameter ensures that appropriate messages are displayed if a virus is found.

Responsibility: System Administrator

Check Content:
From the Symantec Enterprise Server- Symantec System Center Console - select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Scheduled Scans -> Highlight the client server weekly scan -> select Edit -> select Scan Settings -> select Notifications -> Ensure “Display notification message on infected computer” is selected.

Criteria: If “Display notification message on infected computer” is selected, this is not a finding.

To make this determination on the client machine, navigate to the following registry key:
HKLM\Software\Intel\Landesk\VirusProtect6\CurrentVersion\LocalScans\ClientServerScheduledScan_1.
Note: In the key ClientServerScheduledScan_1, the 1 indicates the entry number for the scan. It may be necessary to review all ClientServerScheduledScan_X keys in the LocalScans branch to evaluate this check.

Criteria: If the value of MessageBox is 1, this is not a finding.

Fix Text: From the Symantec Enterprise Server- Symantec System Center Console - select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Scheduled Scans -> Highlight the client server weekly scan -> select Edit -> select Scan Settings -> select Notifications -> select “Display notification message on infected computer”.

Group ID (Vulid): V-6390
Group Title: DTAS042-Symantec Antivirus weekly scan exclude fil
Rule ID: SV-21059r1_rule
Severity: CAT II
Rule Version (STIG-ID): DTAS042
Rule Title: The Symantec Antivirus weekly scan parameter for exclude files is incorrect.

Vulnerability Discussion: This parameter controls which files are excluded from the weekly scan.

Responsibility: System Administrator

Check Content:
From the Symantec Enterprise Server- Symantec System Center Console - select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Scheduled Scans -> Highlight the client server weekly scan -> select Edit -> select Scan Settings -> Ensure that “Exclude files and folders” is unchecked.

Note: If “Exclude files and folders” is checked, select the Exclusions tab File/Folders button and validate that no local drives are being excluded from the scan.

Criteria: If the “Exclude files and folders” is not selected, this is not a finding.

To make this determination on the client machine, navigate to the following registry key:
HKLM\Software\Intel\Landesk\VirusProtect6\CurrentVersion\LocalScans\ClientServerScheduledScan_1.
Note: In the key ClientServerScheduledScan_1, the 1 indicates the entry number for the scan. It may be necessary to review all ClientServerScheduledScan_X keys in the LocalScans branch to evaluate this check.

Criteria: If the value of ExcludeByExtensions, HaveExceptionDirs, and HaveExceptionFiles is 0, this is not a finding.

Fix Text: From the Symantec Enterprise Server- Symantec System Center Console - select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Scheduled Scans -> Highlight the client server weekly scan -> select Edit -> select Scan Settings -> check that “Exclude files and folders” is unchecked.
Note: If “Exclude files and folders” is checked, select the Exclusions tab File/Folders button and validate that no local drives are being excluded from the scan.

Group ID (Vulid): V-6395
Group Title: DTAS047-Symantec Antivirus weekly scan compressed
Rule ID: SV-21134r1_rule
Severity: CAT II
Rule Version (STIG-ID): DTAS047
Rule Title: The Symantec Antivirus weekly scan parameter for compressed files is incorrect.

Vulnerability Discussion: This parameter ensures that compressed files are scanned for viruses during the weekly scan.

Responsibility: System Administrator

Check Content:
From the Symantec Enterprise Server- Symantec System Center Console - select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Scheduled Scans -> Highlight the client server weekly scan -> select Edit -> select Scan Settings -> Advanced -> Observe that “Scan files inside compressed files” is selected.

Criteria: If the option “Scan files inside compressed files” is selected, this is not a finding.

To determine this on the client machine, navigate to the following registry key:
HKLM\Software\Intel\Landesk\VirusProtect6\CurrentVersion\LocalScans\ClientServerScheduledScan_1.
Note: In the key ClientServerScheduledScan_1, the 1 indicates the entry number for the scan. It may be necessary to review all ClientServerScheduledScan_X keys in the LocalScans branch to evaluate this check.

Criteria: If the value of ZipFiles is 1, this is not a finding.

Fix Text: From the Symantec Enterprise Server- Symantec System Center Console - select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Scheduled Scans -> Highlight the client server weekly scan -> select Edit -> select Scan Settings -> Advanced -> select “Scan files inside compressed files”.

Group ID (Vulid): V-6396
Group Title: DTAS048-Symantec Antivirus weekly scan backup file
Rule ID: SV-21554r1_rule
Severity: CAT II
Rule Version (STIG-ID): DTAS048
Rule Title: The Symantec Antivirus weekly scan parameter for backup files is incorrect.

Vulnerability Discussion: This parameter controls the action of backing up files to a quarantine area during the weekly scan.

Responsibility: System Administrator

Check Content:
From the Symantec Enterprise Server- Symantec System Center Console - select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Scheduled Scans -> Highlight the client server weekly scan -> select Edit -> select Scan Settings -> Advanced -> Remote Options area, Backup options, ensure that the option for “Backup file before attempting repair” is selected.

Criteria: If the option ““Backup file before attempting repair” is selected, this is not a finding.

To evaluate this on the client machine, navigate to the following key: HKLM\Software\Intel\Landesk\VirusProtect6\CurrentVersion\LocalScans\ClientServerScheduledScan_1.
Note: In the key ClientServerScheduledScan_1, the 1 indicates the entry number for the scan. It may be necessary to review all ClientServerScheduledScan_X keys in the LocalScans branch to evaluate this check.

Criteria: If the value of BackupToQuarantine is 1, this is not a finding.

Fix Text: From the Symantec Enterprise Server- Symantec System Center Console - select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Scheduled Scans -> Highlight the client server weekly scan -> select Edit -> select Scan Settings -> Advanced -> Remote Options area, Backup options, select “Backup file before attempting repair.”

Group ID (Vulid): V-6397
Group Title: DTAS050-Symantec Antivirus weekly scan scan lock
Rule ID: SV-23676r1_rule
Severity: CAT II
Rule Version (STIG-ID): DTAS050
Rule Title: The Symantec Antivirus weekly scan parameter for scan lock is incorrect.

Vulnerability Discussion: This parameter ensures that users cannot stop the weekly scan.

Responsibility: System Administrator

Check Content:
From the Symantec Enterprise Server- Symantec System Center Console - select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Scheduled Scans -> Highlight the client server weekly scan -> select Edit -> select Scan Settings -> Advanced -> in Remote Options area, ensure “Allow user to stop scan” is unchecked.

Criteria: If the option for “Allow user to stop scan" is not selected, this is not a finding.

To evaluate this check on the client machine, navigate to the following registry key: HKLM\Software\Intel\Landesk\VirusProtect6\CurrentVersion\LocalScans\ClientServerScheduledScan_1.
Note: In the key ClientServerScheduledScan_1, the 1 indicates the entry number for the scan. It may be necessary to

review all ClientServerScheduledScan_X keys in the LocalScans branch to evaluate this check.

Criteria: If the value of ScanLocked is 1, this is not a finding.

Fix Text: From the Symantec Enterprise Server- Symantec System Center Console - select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Scheduled Scans -> Highlight the client server weekly scan -> select Edit -> select Scan Settings -> Advanced -> In the Remote Options area, ensure that “Allow user to stop scan” is unchecked.

Group ID (Vulid): V-14477
Group Title: DTAS060-Symantec Antivirus autoprotect Block Risks
Rule ID: SV-21062r1_rule
Severity: CAT II
Rule Version (STIG-ID): DTAS060
Rule Title: The Symantec Antivirus autoprotect parameter for Block Security Risks is incorrect.

Vulnerability Discussion: The parameter checks and blocks various types of spyware. Without the correct setting, the program will not block the various types of spyware.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\ INTEL\LANDesk\VirusProtect6\CurrentVersion\
Storages\Filesystem\RealTimeScan
Criteria: If the value of APBlockingSecurityRisks is 1, this is not a finding.
This check applies to version 10.x only.

Check Content:
From the Symantec Enterprise Server, Symantec System Center Console: select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Client Auto-Protect Options -> File System tab -> Ensure the option “Block security risks” is selected.

Criteria: If the option “Block security risks” is selected, this is not a finding.

Fix Text: From the Symantec Enterprise Server, Symantec System Center Console: select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Client Auto-Protect Options -> File System tab -> in the Options area, select “Block security risks”.

Group ID (Vulid): V-14481
Group Title: DTAS061-Symantec Antivirus autoprotect Scan Risks
Rule ID: SV-21063r1_rule
Severity: CAT II
Rule Version (STIG-ID): DTAS061
Rule Title: The Symantec Antivirus autoprotect parameter for scan for security risks is incorrect.

Vulnerability Discussion: The AntiVirus has a security risk policy that can be modified/customized for each site. Without Auto-Protect running, these risk polices cannot be scanned and the risk detected.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\ INTEL\LANDesk\VirusProtect6\CurrentVersion\
Storages\Filesystem\RealTimeScan
Criteria: If the value of RespondToThreats is 3, this is not a finding.
This check applies to version 10.x only.

Check Content:
From the Symantec Enterprise Server, Symantec System Center Console: select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Client Auto-Protect Options -> File System tab -> Ensure the option “Scan for security risks” is selected.

Criteria: If the option “Scan for security risks” is selected, this is not a finding.

Fix Text: From the Symantec Enterprise Server, Symantec System Center Console: select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Client Auto-Protect Options -> File System tab -> in the Options area, select “Scan for security risks”.

Group ID (Vulid): V-14482
Group Title: DTAS062-Symantec Antivirus autoprotect Delete Infe
Rule ID: SV-21064r1_rule
Severity: CAT II
Rule Version (STIG-ID): DTAS062
Rule Title: The Symantec Antivirus autoprotect parameter for Delete Infected Files on Creation is incorrect.

Vulnerability Discussion: The Symantec Antivirus autoprotect parameter for Delete Infected Files on Creation is incorrect.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\ INTEL\LANDesk\VirusProtect6\CurrentVersion\
Storages\Filesystem\RealTimeScan
Criteria: If the value of DeleteInfectedOnCreate is 1, this is not a finding.
This check applies to version 10.x only.

Check Content:
From the Symantec Enterprise Server, Symantec System Center Console: select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Client Auto-Protect Options -> File System tab -> Advanced -> in the Scan files when area, ensure the option “For Leave Alone (Log only), delete infected files on creation” is selected.

Criteria: If the option “For Leave Alone (Log only), delete infected files on creation” is selected, this is not a finding.

Fix Text: From the Symantec Enterprise Server, Symantec System Center Console: select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Client Auto-Protect Options -> File System tab -> Advanced -> in the Scan files when area, select “For Leave Alone (Log only), delete infected files on creation”.

Group ID (Vulid): V-14591
Group Title: DTAS063-Symantec Antivirus autoprotect Threattrace
Rule ID: SV-21065r1_rule
Severity: CAT II
Rule Version (STIG-ID): DTAS063
Rule Title: The Symantec AntiVirus Auto-Protect parameter for Threat Tracer is incorrect.

Vulnerability Discussion: Threat Tracer, provides insight into a threat source.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\ INTEL\LANDesk\VirusProtect6\CurrentVersion\
Storages\Filesystem\RealTimeScan
Criteria: If the value of ThreatTracerOnOff is 1, this is not a finding.
This check applies to version 10.x only.

Check Content:
From the Symantec Enterprise Server, Symantec System Center Console: select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Client Auto-Protect Options -> File System tab -> Advanced -> in the Risk Tracer area, ensure the option “Enable Risk Tracer” is selected.

Criteria: If the option “Enable Risk Tracer” is selected, this is not a finding.

Fix Text: From the Symantec Enterprise Server, Symantec System Center Console: select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Client Auto-Protect Options -> File System tab -> Advanced -> in the Risk Tracer area, select “Enable Risk Tracer”.

Group ID (Vulid): V-14592
Group Title: DTAS064-Symantec Antivirus autoprotect Bloodhound
Rule ID: SV-21066r1_rule
Severity: CAT II
Rule Version (STIG-ID): DTAS064
Rule Title: The Symantec Antivirus autoprotect parameter for Bloodhound technology is incorrect.

Vulnerability Discussion: Bloodhound Virus detection scans outgoing email messages helps to prevent the spread of threats such as worms that can use email clients to replicate and distribute themselves across a network.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\ INTEL\LANDesk\VirusProtect6\CurrentVersion\
Storages\Filesystem\RealTimeScan
Criteria: If the value of Heuristics is 1, this is not a finding.
This check applies to version 10.x only.

Check Content:
From the Symantec Enterprise Server, Symantec System Center Console: select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Client Auto-Protect Options -> File System tab -> Advanced -> in the Additional advanced options area, select

Heuristics -> Ensure that “Enable Bloodhound™ virus detection technology” is selected.

Criteria: If the option “Enable Bloodhound™ virus detection technology” is selected, this is not a finding.

Fix Text: From the Symantec Enterprise Server, Symantec System Center Console: select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Client Auto-Protect Options -> File System tab -> Advanced -> in the Additional advanced options area, select Heuristics -> select “Enable Bloodhound™ virus detection technology”.

Group ID (Vulid): V-14593
Group Title: DTAS065-Symantec Antivirus autoprotect Heuristic
Rule ID: SV-21135r1_rule
Severity: CAT II
Rule Version (STIG-ID): DTAS065
Rule Title: The Symantec Antivirus autoprotect parameter for Heuristics Level is incorrect.

Vulnerability Discussion: Heuristics analyzes a program's structure, its behavior, and other attributes for virus-like characteristics. In many cases, it can protect against threats such as mass-mailing worms and macro viruses, if you encounter them before updating your virus definitions. Advanced heuristics looks for script-based threats in HTML, VBScript, and JavaScript files.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\ INTEL\LANDesk\VirusProtect6\CurrentVersion\
Storages\Filesystem\RealTimeScan
Criteria: If the value of HeuristicsLevel is 2 or 3, this is not a finding.
This check applies to version 10.x only.

Check Content:
From the Symantec Enterprise Server, Symantec System Center Console: select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Client Auto-Protect Options -> File System tab -> Advanced -> in the Additional advanced options area, select Heuristics -> Ensure that “Default level of protection” or “Maximum level of protection” is selected.

Criteria: If the options “Default level of protection” or “Maximum level of protection” is selected, this is not a finding.

Fix Text: From the Symantec Enterprise Server, Symantec System Center Console: select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Client Auto-Protect Options -> File System tab -> Advanced -> in the Additional advanced options area, select Heuristics -> select “Default level of protection” or “Maximum level of protection”.

Group ID (Vulid): V-14594
Group Title: DTAS066-Symantec Antivirus autoprotect MacroFirst
Rule ID: SV-23677r1_rule
Severity: CAT II
Rule Version (STIG-ID): DTAS066
Rule Title: The Symantec Antivirus autoprotect parameter for macro virus first action is incorrect.

Vulnerability Discussion: This setting is required for the Auto-Protect Macro virus First action policy. When a Macro virus is detected, the first action to be performed must be the option to delete risk, clean risk, or quarantine the risk.

Responsibility: Information Assurance Officer

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\ INTEL\LANDesk\VirusProtect6\CurrentVersion\
Storages\Filesystem\RealTimeScan
Criteria: If the value of FirstMacroAction is 1, 3 or 5, this is not a finding.

Check Content:
From the Symantec Enterprise Server- Symantec System Center Console - select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Client Auto-Protect Options -> File System tab -> -> Actions -> Highlight Macro virus -> Ensure for First action: Clean risk, Quarantine risk, or Delete risk is selected.

Criteria: If the options selected for Macro virus First action are Clean risk, Quarantine risk, or Delete risk, this is not a finding.

Fix Text: From the Symantec Enterprise Server- Symantec System Center Console - select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Client Auto-Protect Options -> File System tab -> Actions -> Highlight Macro virus: First action:, select "Clean risk, Quarantine risk, or Delete risk".

Group ID (Vulid): V-14595
Group Title: DTAS067-Symantec Antivirus autoprotect MacroSecond
Rule ID: SV-21068r1_rule
Severity: CAT II
Rule Version (STIG-ID): DTAS067
Rule Title: The Symantec Antivirus autoprotect parameter for macro virus second action is incorrect.

Vulnerability Discussion: A program or code segment written in the internal macro language of an application. Some macros replicate, while others infect documents.
After the first iteration, the file Book1 is inserted in the Excel Start directory to make sure that any newly opened files become infected.

The virus then starts a second iteration through all workbooks and macros. During this second iteration any uninfected files are infected.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\ INTEL\LANDesk\VirusProtect6\CurrentVersion\
Storages\Filesystem\RealTimeScan
Criteria: If the value of SecondMacroAction is 1,3 or 5, this is not a finding.

Check Content:
From the Symantec Enterprise Server- Symantec System Center Console - select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -

> Client Auto-Protect Options -> File System tab -> Actions -> Highlight Macro virus: Ensure for If first action fails: Clean risk, Quarantine risk, or Delete risk is selected.

Criteria: If the options selected for Macro virus If first action fails are Clean risk, Quarantine risk, or Delete risk, this is not a finding.

Fix Text: From the Symantec Enterprise Server- Symantec System Center Console - select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Client Auto-Protect Options -> File System tab -> Actions -> Highlight Macro virus: If first action fails:, select "Clean risk, Quarantine risk, or Delete risk".

Group ID (Vulid): V-14596
Group Title: DTAS068-Symantec Antivirus autoprotect Nonmacro fi
Rule ID: SV-21069r1_rule
Severity: CAT II
Rule Version (STIG-ID): DTAS068
Rule Title: The Symantec Antivirus autoprotect parameter for non-macro first action virus is incorrect.

Vulnerability Discussion: A program or code segment written in the internal macro language of an application. Some macros replicate, while others infect documents.
After the first iteration, the file Book1 is inserted in the Excel Start directory to make sure that any newly opened files become infected.

The virus then starts a second iteration through all workbooks and macros. During this second iteration any uninfected files are infected.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\ INTEL\LANDesk\VirusProtect6\CurrentVersion\
Storages\Filesystem\RealTimeScan

Criteria: If the value of FirstAction is 1,3, or 5, this is not a finding

Check Content:
From the Symantec Enterprise Server- Symantec System Center Console - select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Client Auto-Protect Options -> File System tab -> Actions -> Highlight Non-Macro Virus: Ensure for First Action: Clean risk, Quarantine risk, or Delete risk is selected.

Criteria: If the options selected for Non-Macro virus First action are Clean risk, Quarantine risk, or Delete risk, this is not a finding.

Fix Text: From the Symantec Enterprise Server- Symantec System Center Console - select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Client Auto-Protect Options -> File System tab -> Actions -> Highlight Non-Macro Virus: First Action:, select "Clean risk, Quarantine risk, or Delete risk".

Group ID (Vulid): V-14597
Group Title: DTAS069-Symantec Antivirus autoprotect Nonmacro se
Rule ID: SV-21070r1_rule
Severity: CAT II
Rule Version (STIG-ID): DTAS069
Rule Title: The Symantec Antivirus autoprotect parameter for check non-macro second action is incorrect.

Vulnerability Discussion: A program or code segment written in the internal macro language of an application. Some macros replicate, while others infect documents.
After the first iteration, the file Book1 is inserted in the Excel Start directory to make sure that any newly opened files become infected.

The virus then starts a second iteration through all workbooks and macros. During this second iteration any uninfected files are infected.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\ INTEL\LANDesk\VirusProtect6\CurrentVersion\
Storages\Filesystem\RealTimeScan
Criteria: If the value of SecondAction is 1,3, or 5, this is not a finding.

Check Content:
From the Symantec Enterprise Server- Symantec System Center Console - select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Client Auto-Protect Options -> File System tab -> Actions -> Highlight Non-macro virus: Edit for If first action fails: Clean risk, Quarantine risk, or Delete risk is selected.

Criteria: If the options selected for Non-Macro virus If first action fails are Clean risk, Quarantine risk, or Delete risk, this is not a finding.

Fix Text: From the Symantec Enterprise Server- Symantec System Center Console - select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Client Auto-Protect Options -> File System tab -> Actions -> Highlight Non-macro virus: If first action fails:, select "Clean risk, Quarantine risk, or Delete risk".

Group ID (Vulid): V-14598
Group Title: DTAS070-Symantec Antivirus autoprotect risks first
Rule ID: SV-23678r1_rule
Severity: CAT II
Rule Version (STIG-ID): DTAS070
Rule Title: The Symantec Antivirus autoprotect parameter for Security Risks first action is incorrect.

Vulnerability Discussion: This setting is required for the Auto-Protect Security Risks First action policy. When a Security Risk is detected, the first action to be performed must be the option to delete risk, clean risk, or quarantine the risk.

Responsibility: System Administrator

Check Content:

Procedure: This is a multiple step process to ensure compliance. Non-compliance points are identified throughout the procedures.
Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\ INTEL\LANDesk\VirusProtect6\CurrentVersion\
Storages\Filesystem\RealTimeScan\Expanded
Criteria: If the value of FirstAction is not 1 or 3, this is a finding.
If the value FirstAction is 1 or 3, then check each of the following steps. Each of the 8 parts (A-H) must be in compliance for the vulnerability to be considered not a finding.
A - If the value of OverrideDefaultActions within HKLM\Software\ INTEL\LANDesk\VirusProtect6 \CurrentVersion\Storages\Filesystem\RealTimeScan\Expanded\TCID-10
If the value is 0 or the value is not there, this part is compliant.
If the value is 1, then check the FirstAction value within HKLM\Software\ INTEL\LANDesk\VirusProtect6 \CurrentVersion\Storages\Filesystem\RealTimeScan\Expanded\TCID-10
If the value is 1 or 3, this is compliant, otherwise this is a finding.
B - If the value of OverrideDefaultActions within HKLM\Software\ INTEL\LANDesk\VirusProtect6 \CurrentVersion\Storages\Filesystem\RealTimeScan\Expanded\TCID-11
If the value is 0 or the value is not there, this part is compliant.
If the value is 1, then check the FirstAction within HKLM\Software\ INTEL\LANDesk\VirusProtect6 \CurrentVersion\Storages\Filesystem\RealTimeScan\Expanded\TCID-11
If the value is 1 or 3, this is compliant, otherwise this is a finding.
C - If the value of OverrideDefaultActions within HKLM\Software\ INTEL\LANDesk\VirusProtect6 \CurrentVersion\Storages\Filesystem\RealTimeScan\Expanded\TCID-4
If the value is 0 or the value is not there, this part is compliant.
If the value is 1, then check the FirstAction within HKLM\Software\ INTEL\LANDesk\VirusProtect6 \CurrentVersion\Storages\Filesystem\RealTimeScan\Expanded\TCID-4
If the value is 1 or 3, this is compliant, otherwise this is a finding.
D - If the value of OverrideDefaultActions within HKLM\Software\ INTEL\LANDesk\VirusProtect6 \CurrentVersion\Storages\Filesystem\RealTimeScan\Expanded\TCID-5
If the value is 0 or the value is not there, this part is compliant.
If the value is 1, then check the FirstAction within HKLM\Software\ INTEL\LANDesk\VirusProtect6 \CurrentVersion\Storages\Filesystem\RealTimeScan\Expanded\TCID-5
If the value is 1 or 3, this is compliant, otherwise this is a finding.
E - If the value of OverrideDefaultActions within HKLM\Software\ INTEL\LANDesk\VirusProtect6 \CurrentVersion\Storages\Filesystem\RealTimeScan\Expanded\TCID-6
If the value is 0 or the value is not there, this part is compliant.
If the value is 1, then check the FirstAction within HKLM\Software\ INTEL\LANDesk\VirusProtect6 \CurrentVersion\Storages\Filesystem\RealTimeScan\Expanded\TCID-6
If the value is 1 or 3, this is compliant, otherwise this is a finding.
F - If the value of OverrideDefaultActions within HKLM\Software\ INTEL\LANDesk\VirusProtect6 \CurrentVersion\Storages\Filesystem\RealTimeScan\Expanded\TCID-7
If the value is 0 or the value is not there, this part is compliant.
If the value is 1, then check the FirstAction within HKLM\Software\ INTEL\LANDesk\VirusProtect6 \CurrentVersion\Storages\Filesystem\RealTimeScan\Expanded\TCID-7
If the value is 1 or 3, this is compliant, otherwise this is a finding.
G - If the value of OverrideDefaultActions within HKLM\Software\ INTEL\LANDesk\VirusProtect6 \CurrentVersion\Storages\Filesystem\RealTimeScan\Expanded\TCID-8
If the value is 0 or the value is not there, this part is compliant.
If the value is 1, then check the FirstAction within HKLM\Software\ INTEL\LANDesk\VirusProtect6 \CurrentVersion\Storages\Filesystem\RealTimeScan\Expanded\TCID-8
If the value is 1 or 3, this is compliant, otherwise this is a finding.
H - If the value of OverrideDefaultActions within HKLM\Software\ INTEL\LANDesk\VirusProtect6 \CurrentVersion\Storages\Filesystem\RealTimeScan\Expanded\TCID-9
If the value is 0 or the value is not there, this part is compliant.
If the value is 1, then check the FirstAction within HKLM\Software\ INTEL\LANDesk\VirusProtect6 \CurrentVersion\Storages\Filesystem\RealTimeScan\Expanded\TCID-9
If the value is 1 or 3, this is compliant, otherwise this is a finding.

Check Content:
Procedure: This is a multiple step process. Non-compliance points are identified throughout the procedures.

From the Symantec Enterprise Server- Symantec System Center Console - select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Client Auto-Protect Options -> File System tab -> Actions -> highlight Security Risks: observe option for First action.

Criteria: If the option selected for Security Risks First action is not “Quarantine risk” or “Delete risk”, this is a finding.

If the selection for First action is “Quarantine risk” or “Delete risk”, continue with each of the following steps. Each of the 8 parts (A – H) must be in compliance for the vulnerability to be considered not a finding.

A. Highlight Adware

If Override actions configured for Security Risks is not checked, this part is compliant.

If Override actions configured for Security Risks is checked: for First action if Quarantine risk or Delete risk are selected, this is compliant, otherwise this is a finding.

B. Highlight Dialers

If Override actions configured for Security Risks is not checked, this part is compliant.

If Override actions configured for Security Risks is checked: for First action if Quarantine risk or Delete risk are selected, this is compliant, otherwise this is a finding.

C. Highlight Hack Tools

If Override actions configured for Security Risks is not checked, this part is compliant.

If Override actions configured for Security Risks is checked: for First action if Quarantine risk or Delete risk are selected, this is compliant, otherwise this is a finding.

D. Highlight Joke Programs

If Override actions configured for Security Risks is not checked, this part is compliant.

If Override actions configured for Security Risks is checked: for First action if Quarantine risk or Delete risk are selected, this is compliant, otherwise this is a finding.

E. Highlight Other

If Override actions configured for Security Risks is not checked, this part is compliant.

If Override actions configured for Security Risks is checked: for First action if Quarantine risk or Delete risk are selected, this is compliant, otherwise this is a finding.

F. Highlight Remote Access

If Override actions configured for Security Risks is not checked, this part is compliant.

If Override actions configured for Security Risks is checked: for First action if Quarantine risk or Delete risk are selected, this is compliant, otherwise this is a finding.

G. Highlight Spyware

If Override actions configured for Security Risks is not checked, this part is compliant.

If Override actions configured for Security Risks is checked: for First action if Quarantine risk or Delete risk are selected, this is compliant, otherwise this is a finding.

H. Highlight Trackware

If Override actions configured for Security Risks is not checked, this part is compliant.

If Override actions configured for Security Risks is checked: for First action if Quarantine risk or Delete risk are selected, this is compliant, otherwise this is a finding.

Fix Text: From the Symantec Enterprise Server- Symantec System Center Console - select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Client Auto-Protect Options -> File System tab -> Actions -> Highlight Security Risks: under the Actions tab First action, select one of the following, “Quarantine risk” or “Delete risk”.

If the selection for First action is “Quarantine risk” or “Delete risk”, continue with each of the following steps. Each of the 8 parts (A – H) must be in compliance for the vulnerability to be considered not a finding.

A. Highlight Adware - if Override actions configured for Security Risks is checked, for First action, select Quarantine risk or Delete risk.

B. Highlight Dialers - if Override actions configured for Security Risks is checked, for First action, select Quarantine risk or Delete risk.

C. Highlight Hack Tools – if Override actions configured for Security Risks is checked, for First action, select Quarantine risk or Delete risk.

D. Highlight Joke Programs – if Override actions configured for Security Risks is checked, for First action, select Quarantine risk or Delete risk.

E. Highlight Other – if Override actions configured for Security Risks is checked, for First action, select Quarantine risk or Delete risk.

F. Highlight Remote Access – if Override actions configured for Security Risks is checked, for First action, select Quarantine risk or Delete risk.

G. Highlight Spyware – if Override actions configured for Security Risks is checked, for First action, select Quarantine risk or Delete risk.

H. Highlight Trackware - if Override actions configured for Security Risks is checked, for First action, select Quarantine risk or Delete risk.

Group ID (Vulid): V-14600
Group Title: DTAS071-Symantec Antivirus autoprotect Risk Second
Rule ID: SV-23680r1_rule
Severity: CAT II
Rule Version (STIG-ID): DTAS071
Rule Title: The Symantec Antivirus autoprotect parameter for Security Risks Second Action is incorrect.

Vulnerability Discussion: This setting is required for the Auto-Protect Security Risks second ("If first action

fails") action policy, When a Security Risk, such as Adware or Dialers, is detected, the second action to be performed must be the option to delete risk or quarantine the risk.

Responsibility: System Administrator

Check Content:
Procedure: This is a multiple step process to ensure compliance. Non-compliance points are identified throughout the procedures.
Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\ INTEL\LANDesk\VirusProtect6\CurrentVersion\
Storages\Filesystem\RealTimeScan\Expanded
Criteria: If the value of SecondAction is not 1 or 3, this is a finding.
If the value SecondAction is 1 or 3 then check each of the following steps. Each of the 8 parts (A-H) must be in compliance for the vulnerability to be considered not a finding.
A - If the value of OverrideDefaultActions within HKLM\Software\ INTEL\LANDesk\VirusProtect6
\CurrentVersion\Storages\Filesystem\RealTimeScan\Expanded\TCID-10
If the value is 0 or the value is not there, this part is compliant.
If the value is 1, then check the SecondAction within HKLM\Software\
INTEL\LANDesk\VirusProtect6
\CurrentVersion\Storages\Filesystem\RealTimeScan\Expanded\TCID-10
If the value is 1 or 3, this is compliant, otherwise this is a finding.
B - If the value of OverrideDefaultActions within HKLM\Software\ INTEL\LANDesk\VirusProtect6
\CurrentVersion\Storages\Filesystem\RealTimeScan\Expanded\TCID-11
If the value is 0 or the value is not there, this part is compliant.
If the value is 1, then check the SecondAction within HKLM\Software\
INTEL\LANDesk\VirusProtect6
\CurrentVersion\Storages\Filesystem\RealTimeScan\Expanded\TCID-11
If the value is 1 or 3, this is compliant, otherwise this is a finding.
C - If the value of OverrideDefaultActions within HKLM\Software\ INTEL\LANDesk\VirusProtect6
\CurrentVersion\Storages\Filesystem\RealTimeScan\Expanded\TCID-4
If the value is 0 or the value is not there, this part is compliant.
If the value is 1, then check the SecondAction within HKLM\Software\
INTEL\LANDesk\VirusProtect6
\CurrentVersion\Storages\Filesystem\RealTimeScan\Expanded\TCID-4
If the value is 1 or 3, this is compliant, otherwise this is a finding.
D - If the value of OverrideDefaultActions within HKLM\Software\ INTEL\LANDesk\VirusProtect6
\CurrentVersion\Storages\Filesystem\RealTimeScan\Expanded\TCID-5
If the value is 0 or the value is not there, this part is compliant.
If the value is 1, then check the SecondAction within HKLM\Software\
INTEL\LANDesk\VirusProtect6
\CurrentVersion\Storages\Filesystem\RealTimeScan\Expanded\TCID-5
If the value is 1 or 3, this is compliant, otherwise this is a finding.
E - If the value of OverrideDefaultActions within HKLM\Software\ INTEL\LANDesk\VirusProtect6
\CurrentVersion\Storages\Filesystem\RealTimeScan\Expanded\TCID-6
If the value is 0 or the value is not there, this part is compliant.
If the value is 1, then check the SecondAction within HKLM\Software\
INTEL\LANDesk\VirusProtect6
\CurrentVersion\Storages\Filesystem\RealTimeScan\Expanded\TCID-6
If the value is 1 or 3, this is compliant, otherwise this is a finding.
F - If the value of OverrideDefaultActions within HKLM\Software\ INTEL\LANDesk\VirusProtect6
\CurrentVersion\Storages\Filesystem\RealTimeScan\Expanded\TCID-7
If the value is 0 or the value is not there, this part is compliant.
If the value is 1, then check the SecondAction within HKLM\Software\
INTEL\LANDesk\VirusProtect6
\CurrentVersion\Storages\Filesystem\RealTimeScan\Expanded\TCID-7
If the value is 1 or 3, this is compliant, otherwise this is a finding.
G - If the value of OverrideDefaultActions within HKLM\Software\ INTEL\LANDesk\VirusProtect6

\CurrentVersion\Storages\Filesystem\RealTimeScan\Expanded\TCID-8
If the value is 0 or the value is not there, this part is compliant.
If the value is 1, then check the SecondAction within HKLM\Software\
INTEL\LANDesk\VirusProtect6
\CurrentVersion\Storages\Filesystem\RealTimeScan\Expanded\TCID-8
If the value is 1 or 3, this is compliant, otherwise this is a finding.
H - If the value of OverrideDefaultActions within HKLM\Software\ INTEL\LANDesk\VirusProtect6
\CurrentVersion\Storages\Filesystem\RealTimeScan\Expanded\TCID-9
If the value is 0 or the value is not there, this part is compliant.
If the value is 1, then check the SecondAction within HKLM\Software\
INTEL\LANDesk\VirusProtect6
\CurrentVersion\Storages\Filesystem\RealTimeScan\Expanded\TCID-9
If the value is 1 or 3, this is compliant, otherwise this is a finding.

Check Content:
Procedure: This is a multiple step process. Non-compliance points are identified throughout the procedures.

From the Symantec Enterprise Server- Symantec System Center Console - select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Client Auto-Protect Options -> File System tab -> Actions -> highlight Security Risks: observe option for If first action fails.

Criteria: If the option selected for Security Risks First action is not “Quarantine risk” or “Delete risk”, this is a finding.

If the selection for If first action fails is “Quarantine risk” or “Delete risk”, continue with each of the following steps. Each of the 8 parts (A – H) must be in compliance for the vulnerability to be considered not a finding.

A. Highlight Adware

If Override actions configured for Security Risks is not checked, this part is compliant.

If Override actions configured for Security Risks is checked: for If first action fails if Quarantine risk or Delete risk are selected, this is compliant, otherwise this is a finding.

B. Highlight Dialers

If Override actions configured for Security Risks is not checked, this part is compliant.

If Override actions configured for Security Risks is checked: for If first action fails if Quarantine risk or Delete risk are selected, this is compliant, otherwise this is a finding.

C. Highlight Hack Tools

If Override actions configured for Security Risks is not checked, this part is compliant.

If Override actions configured for Security Risks is checked: for If first action fails if Quarantine risk or Delete risk are selected, this is compliant, otherwise this is a finding.

D. Highlight Joke Programs

If Override actions configured for Security Risks is not checked, this part is compliant.

If Override actions configured for Security Risks is checked: for If first action fails if Quarantine risk or Delete risk are selected, this is compliant, otherwise this is a finding.

E. Highlight Other

If Override actions configured for Security Risks is not checked, this part is compliant.

If Override actions configured for Security Risks is checked: for If first action fails if Quarantine risk or Delete risk are selected, this is compliant, otherwise this is a finding.

F. Highlight Remote Access

If Override actions configured for Security Risks is not checked, this part is compliant.

If Override actions configured for Security Risks is checked: for If first action fails if Quarantine risk or Delete risk are selected, this is compliant, otherwise this is a finding.

G. Highlight Spyware

If Override actions configured for Security Risks is not checked, this part is compliant.

If Override actions configured for Security Risks is checked: for If first action fails if Quarantine risk or Delete risk are selected, this is compliant, otherwise this is a finding.

H. Highlight Trackware

If Override actions configured for Security Risks is not checked, this part is compliant.

If Override actions configured for Security Risks is checked: for If first action fails if Quarantine risk or Delete risk are selected, this is compliant, otherwise this is a finding.

Fix Text: From the Symantec Enterprise Server- Symantec System Center Console - select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Client Auto-Protect Options -> File System tab -> Actions -> Highlight Security Risks: under the Actions tab If first action fails: select one of the following “Quarantine risk” or “Delete risk”.

If the selection for If first action fails is “Quarantine risk” or “Delete risk”, continue with each of the following steps. Each of the 8 parts (A – H) must be in compliance for the vulnerability to be considered not a finding.

A. Highlight Adware - if Override actions configured for Security Risks is checked, for If first action fails, select Quarantine risk or Delete risk.

B. Highlight Dialers - if Override actions configured for Security Risks is checked, for If first action fails, select Quarantine risk or Delete risk.

C. Highlight Hack Tools – if Override actions configured for Security Risks is checked, for If first action fails, select Quarantine risk or Delete risk.

D. Highlight Joke Programs – if Override actions configured for Security Risks is checked, for If first action fails, select Quarantine risk or Delete risk.

E. Highlight Other – if Override actions configured for Security Risks is checked, for If first action fails, select Quarantine risk or Delete risk.

F. Highlight Remote Access – if Override actions configured for Security Risks is checked, for If first action fails, select Quarantine risk or Delete risk.

G. Highlight Spyware – if Override actions configured for Security Risks is checked, for If first action fails, select Quarantine risk or Delete risk.

H. Highlight Trackware - if Override actions configured for Security Risks is checked, for If first action fails, select Quarantine risk or Delete risk.

Group ID (Vulid): V-14601
Group Title: DTAS080-Symantec Antivirus email client Notificati
Rule ID: SV-23681r1_rule
Severity: CAT II
Rule Version (STIG-ID): DTAS080
Rule Title: The Symantec Antivirus email client for notification into the email is incorrect.

Vulnerability Discussion: This setting is required in order for the Symantec Antivirus email client to send an email warning notification of a security risk. The “Insert warning into e-mail message” attribute must be selected.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\ INTEL\LANDesk\VirusProtect6\CurrentVersion\
Storages\EmailName\RealTimeScan
Criteria: If the value of InsertWarning is 1, this is not a finding.
Note: This check is for Email clients. Substitute your email application name (InternetMail, LotusNotes, or MicrosoftExchangeClient) into the registry string indicated by EmailName.
If email client is not installed this check is NA.

Check Content:
From the Symantec Enterprise Server, Symantec System Center Console: select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Client Auto-Protect Options -> email name tab (where “email name” is the email client type; options are Internet E-mail, Lotus Notes, and Microsoft Exchange) -> Ensure “Insert warning into e-mail message” is selected.

Criteria: If the option “Insert warning into e-mail message” is selected, this is not a finding.

Fix Text: From the Symantec Enterprise Server, Symantec System Center Console: select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Client Auto-Protect Options -> email name tab (where “email name” is the email client type; options are Internet E-mail, Lotus Notes, or Microsoft Exchange) -> In the E-mail Messages area, select “Insert warning into e-mail message”.

Group ID (Vulid): V-14602
Group Title: DTAS081- Symantec Antivirus autoprotect macro firs
Rule ID: SV-23687r1_rule
Severity: CAT II
Rule Version (STIG-ID): DTAS081
Rule Title: The Symantec Antivirus autoprotect email parameter for macro virus first action is incorrect.

Vulnerability Discussion: This setting is required for the Auto-Protect email parameter Macro virus First action policy. When an email Macro virus is detected, the first action to be performed must be the option to delete risk, clean risk, or quarantine the risk.

Responsibility: System Administrator

Check Content:

Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\ INTEL\LANDesk\VirusProtect6\CurrentVersion\
Storages\EmailName\RealTimeScan
Criteria: If the value of FirstMacroAction is 1, 3 or 5, this is not a finding.
Note: This check is for email clients. Substitute your email application name (InternetMail, LotusNotes, or MicrosoftExchangeClient) into the registry string indicated by EmailName.
If email client is not installed, this check is NA.

Check Content:
From the Symantec Enterprise Server, Symantec System Center Console: select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Client Auto-Protect Options -> email name tab (where “email name” is the email client type; options are Internet E-mail, Lotus Notes, and Microsoft Exchange) -> Actions -> Highlight Macro virus -> Ensure for First action: Clean risk, Quarantine risk, or Delete risk is selected.

Criteria: If the options selected for Macro virus First action are Clean risk, Quarantine risk, or Delete risk, this is not a finding.

Fix Text: From the Symantec Enterprise Server, Symantec System Center Console: select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Client Auto-Protect Options -> email name tab (where “email name” is the email client type; options are Internet E-mail, Lotus Notes, and Microsoft Exchange) -> Actions -> Highlight Macro virus: First action:, select "Clean risk, Quarantine risk, or Delete risk".

Group ID (Vulid): V-14603
Group Title: DTAS082-Symantec Antivirus autoprotect email secon
Rule ID: SV-23688r1_rule
Severity: CAT II
Rule Version (STIG-ID): DTAS082
Rule Title: The Symantec Antivirus autoprotect email parameter for macro virus second action is incorrect.

Vulnerability Discussion: This setting is required for the Auto-Protect email parameter Macro virus second action policy. When an email Macro virus is detected, the second action ("If first action fails:") to be performed must be the option to delete risk, clean risk, or quarantine the risk.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\ INTEL\LANDesk\VirusProtect6\CurrentVersion\
Storages\EmailName\RealTimeScan
Criteria: If the value of SecondMacroAction is 1,3 or 5, this is not a finding.
Note: This check is for email clients. Substitute your email application name (InternetMail, LotusNotes, or MicrosoftExchangeClient) into the registry string indicated by EmailName.
If email client is not installed, this check is NA.
.

Check Content:
From the Symantec Enterprise Server, Symantec System Center Console: select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Client Auto-Protect Options -> email name tab (where “email name” is the email client type; options are Internet E-mail, Lotus Notes, and Microsoft Exchange) -> Actions -> Highlight Macro virus: Ensure for If first action fails: Clean risk, Quarantine risk, or Delete risk is selected.

Criteria: If the options selected for Macro virus If first action fails are Clean risk, Quarantine risk, or Delete risk, this is not a finding.

Fix Text: From the Symantec Enterprise Server, Symantec System Center Console: select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Client Auto-Protect Options -> email name tab (where “email name” is the email client type; options are Internet E-mail, Lotus Notes, and Microsoft Exchange) -> Actions -> Highlight Macro virus: If first action fails:, select "Clean risk, Quarantine risk, or Delete risk".

Group ID (Vulid): V-14604
Group Title: DTAS083-Symantec Antivirus autoprotect email nonma
Rule ID: SV-23689r1_rule
Severity: CAT II
Rule Version (STIG-ID): DTAS083
Rule Title: The Symantec Antivirus autoprotect email parameter for non-macro first action virus is incorrect.

Vulnerability Discussion: This setting is required for the Auto-Protect email parameter non-Macro virus First action policy. When a non-Macro virus is detected, the first action to be performed must be the option to delete risk, clean risk, or quarantine the risk.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\ INTEL\LANDesk\VirusProtect6\CurrentVersion\Storages\EmailName\RealTimeScan
Criteria: If the value of FirstAction is 1,3, or 5, this is not a finding.
Note: This check is for email clients. Substitute your email application name (InternetMail, LotusNotes, or MicrosoftExchangeClient) into the registry string indicated by EmailName.
If email client is not installed, this check is NA.

Check Content:
From the Symantec Enterprise Server, Symantec System Center Console: select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Client Auto-Protect Options -> email name tab (where “email name” is the email client type; options are Internet E-mail, Lotus Notes, and Microsoft Exchange) -> Actions -> Highlight Non-Macro Virus: Ensure for First Action: Clean risk, Quarantine risk, or Delete risk is selected.

Criteria: If the options selected for Non-Macro virus First action are Clean risk, Quarantine risk, or Delete risk, this is not a finding.

Fix Text: From the Symantec Enterprise Server, Symantec System Center Console: select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Client Auto-Protect Options -> email name tab (where “email name” is the email client type; options are Internet E-mail, Lotus Notes, and Microsoft Exchange) -> Actions -> Highlight Non-Macro Virus: First Action:, select "Clean risk, Quarantine risk, or Delete risk".

Group ID (Vulid): V-14605
Group Title: DTAS084-Symantec Antivirus autoprotect email nonma
Rule ID: SV-23691r1_rule
Severity: CAT II
Rule Version (STIG-ID): DTAS084

Rule Title: The Symantec Antivirus autoprotect email parameter for check non-macro second action is incorrect.

Vulnerability Discussion: This setting is required for the Auto-Protect email parameter non-Macro virus Second action policy. When a non-Macro virus is detected the Second action ("If first action fails") to be performed must be the option to delete risk, clean risk, or quarantine the risk.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\ INTEL\LANDesk\VirusProtect6\CurrentVersion\
Storages\EmailName \RealTimeScan
Criteria: If the value of SecondAction is 1,3, or 5, this is not a finding.
Note: This check is for email clients. Substitute your email application name (InternetMail, LotusNotes, or MicrosoftExchangeClient) into the registry string indicated by EmailName.
If email client is not installed, this check is NA.

Check Content:
From the Symantec Enterprise Server, Symantec System Center Console: select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Client Auto-Protect Options -> email name tab (where “email name” is the email client type; options are Internet E-mail, Lotus Notes, and Microsoft Exchange) -> Actions -> Highlight Non-macro virus: Ensure for If first action fails: Clean risk, Quarantine risk, or Delete risk is selected.

Criteria: If the options selected for Non-Macro virus If first action fails are Clean risk, Quarantine risk, or Delete risk, this is not a finding.

Fix Text: From the Symantec Enterprise Server, Symantec System Center Console: select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Client Auto-Protect Options -> email name tab (where “email name” is the email client type; options are Internet E-mail, Lotus Notes, and Microsoft Exchange) -> Actions -> Highlight Non-macro virus: If first action fails:, select "Clean risk, Quarantine risk, or Delete risk".

Group ID (Vulid): V-14606
Group Title: DTAS085-Symantec Antivirus autoprotect email first
Rule ID: SV-23692r1_rule
Severity: CAT II
Rule Version (STIG-ID): DTAS085
Rule Title: The Symantec Antivirus autoprotect email parameter for Security Risks first action is incorrect.

Vulnerability Discussion: This setting is required for the Auto-Protect email Security Risks First action policy. When a Security Risk is detected, the first action to be performed must be the option to delete risk, clean risk, or quarantine the risk.

Responsibility: System Administrator

Check Content:
Procedure: This is a multiple step process to ensure compliance. Non-compliance points are identified throughout the procedures.
Note: This check is for email clients. Substitute your email application name (InternetMail, LotusNotes, or MicrosoftExchangeClient) into the registry string indicated by EmailName.
If email client is not installed, this check is NA.
Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\ INTEL\LANDesk\VirusProtect6\CurrentVersion\

Storages\EmailName \RealTimeScan\Expanded
Criteria: If the value of FirstAction is not 1 or 3, this is a finding.
If the value FirstAction is 1 or 3 then check each of the following steps. Each of the 8 parts (A-H) must be in compliance for the vulnerability to be considered not a finding.
A - If the value of OverrideDefaultActions within HKLM\Software\ INTEL\LANDesk\VirusProtect6 \CurrentVersion\Storages\EmailName \RealTimeScan\Expanded\TCID-10
If the value is 0 or the value is not there, this part is compliant.
If the value is 1, then check the FirstAction within HKLM\Software\ INTEL\LANDesk\VirusProtect6 \CurrentVersion\Storages\EmailName \RealTimeScan\Expanded\TCID-10
If the value is 1 or 3, this is compliant, otherwise this is a finding.
B - If the value of OverrideDefaultActions within HKLM\Software\ INTEL\LANDesk\VirusProtect6 \CurrentVersion\Storages\EmailName \RealTimeScan\Expanded\TCID-11
If the value is 0 or the value is not there, this part is compliant.
If the value is 1, then check the FirstAction within HKLM\Software\ INTEL\LANDesk\VirusProtect6 \CurrentVersion\Storages\EmailName \RealTimeScan\Expanded\TCID-11
If the value is 1 or 3, this is compliant, otherwise this is a finding.
C - If the value of OverrideDefaultActions within HKLM\Software\ INTEL\LANDesk\VirusProtect6 \CurrentVersion\Storages\EmailName \RealTimeScan\Expanded\TCID-4
If the value is 0 or the value is not there, this part is compliant.
If the value is 1, then check the FirstAction within HKLM\Software\ INTEL\LANDesk\VirusProtect6 \CurrentVersion\Storages\EmailName \RealTimeScan\Expanded\TCID-4
If the value is 1 or 3, this is compliant, otherwise this is a finding.
D - If the value of OverrideDefaultActions within HKLM\Software\ INTEL\LANDesk\VirusProtect6 \CurrentVersion\Storages\EmailName \RealTimeScan\Expanded\TCID-5
If the value is 0 or the value is not there, this part is compliant.
If the value is 1, then check the FirstAction within HKLM\Software\ INTEL\LANDesk\VirusProtect6 \CurrentVersion\Storages\EmailName \RealTimeScan\Expanded\TCID-5
If the value is 1 or 3, this is compliant, otherwise this is a finding.
E - If the value of OverrideDefaultActions within HKLM\Software\ INTEL\LANDesk\VirusProtect6 \CurrentVersion\Storages\EmailName \RealTimeScan\Expanded\TCID-6
If the value is 0 or the value is not there, this part is compliant.
If the value is 1, then check the FirstAction within HKLM\Software\ INTEL\LANDesk\VirusProtect6 \CurrentVersion\Storages\EmailName \RealTimeScan\Expanded\TCID-6
If the value is 1 or 3, this is compliant, otherwise this is a finding.
F - If the value of OverrideDefaultActions within HKLM\Software\ INTEL\LANDesk\VirusProtect6 \CurrentVersion\Storages\EmailName \RealTimeScan\Expanded\TCID-7
If the value is 0 or the value is not there, this part is compliant.
If the value is 1, then check the FirstAction within HKLM\Software\ INTEL\LANDesk\VirusProtect6 \CurrentVersion\Storages\EmailName \RealTimeScan\Expanded\TCID-7
If the value is 1 or 3, this is compliant, otherwise this is a finding.
G - If the value of OverrideDefaultActions within HKLM\Software\ INTEL\LANDesk\VirusProtect6 \CurrentVersion\Storages\EmailName \RealTimeScan\Expanded\TCID-8
If the value is 0 or the value is not there, this part is compliant.
If the value is 1, then check the FirstAction within HKLM\Software\ INTEL\LANDesk\VirusProtect6 \CurrentVersion\Storages\EmailName \RealTimeScan\Expanded\TCID-8
If the value is 1 or 3, this is compliant, otherwise this is a finding.
H - If the value of OverrideDefaultActions within HKLM\Software\ INTEL\LANDesk\VirusProtect6 \CurrentVersion\Storages\EmailName \RealTimeScan\Expanded\TCID-9
If the value is 0 or the value is not there, this part is compliant.
If the value is 1, then check the FirstAction within HKLM\Software\ INTEL\LANDesk\VirusProtect6 \CurrentVersion\Storages\EmailName \RealTimeScan\Expanded\TCID-9
If the value is 1 or 3, this is compliant, otherwise this is a finding.

Check Content:
Procedure: This is a multiple step process. Non-compliance points are identified throughout the procedures.

From the Symantec Enterprise Server, Symantec System Center Console: select System Hierarchy -> select

[applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Client Auto-Protect Options -> email name tab (where “email name” is the email client type; options are Internet E-mail, Lotus Notes, and Microsoft Exchange) -> Actions -> highlight Security Risks: observe option for First action:

Criteria: If the option selected for Security Risks First action is not “Quarantine risk” or “Delete risk”, this is a finding.

If the selection for First action is “Quarantine risk” or “Delete risk”, continue with each of the following steps. Each of the 8 parts (A – H) must be in compliance for the vulnerability to be considered not a finding.

A. Highlight Adware

If Override actions configured for Security Risks is not checked, this part is compliant.

If Override actions configured for Security Risks is checked: for First action if Quarantine risk or Delete risk are selected, this is compliant, otherwise this is a finding.

B. Highlight Dialers

If Override actions configured for Security Risks is not checked, this part is compliant.

If Override actions configured for Security Risks is checked: for First action if Quarantine risk or Delete risk are selected, this is compliant, otherwise this is a finding.

C. Highlight Hack Tools

If Override actions configured for Security Risks is not checked, this part is compliant.

If Override actions configured for Security Risks is checked: for First action if Quarantine risk or Delete risk are selected, this is compliant, otherwise this is a finding.

D. Highlight Joke Programs

If Override actions configured for Security Risks is not checked, this part is compliant.

If Override actions configured for Security Risks is checked: for First action if Quarantine risk or Delete risk are selected, this is compliant, otherwise this is a finding.

E. Highlight Other

If Override actions configured for Security Risks is not checked, this part is compliant.

If Override actions configured for Security Risks is checked: for First action if Quarantine risk or Delete risk are selected, this is compliant, otherwise this is a finding.

F. Highlight Remote Access

If Override actions configured for Security Risks is not checked, this part is compliant.

If Override actions configured for Security Risks is checked: for First action if Quarantine risk or Delete risk are selected, this is compliant, otherwise this is a finding.

G. Highlight Spyware

If Override actions configured for Security Risks is not checked, this part is compliant.

If Override actions configured for Security Risks is checked: for First action if Quarantine risk or Delete risk are selected, this is compliant, otherwise this is a finding.

H. Highlight Trackware

If Override actions configured for Security Risks is not checked, this part is compliant.

If Override actions configured for Security Risks is checked: for First action if Quarantine risk or Delete risk are selected, this is compliant, otherwise this is a finding.

Fix Text: From the Symantec Enterprise Server, Symantec System Center Console: select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Client Auto-Protect Options -> email name tab (where “email name” is the email client type; options are Internet E-mail, Lotus Notes, and Microsoft Exchange) -> Actions -> Highlight Security Risks: under the Actions tab First action: select one of the following “Quarantine risk” or “Delete risk”.

If the selection for First action is “Quarantine risk” or “Delete risk”, continue with each of the following steps. Each of the 8 parts (A – H) must be in compliance for the vulnerability to be considered not a finding.

A. Highlight Adware - if Override actions configured for Security Risks is checked, for First action: select Quarantine risk or Delete risk.

B. Highlight Dialers - if Override actions configured for Security Risks is checked, for First action: select Quarantine risk or Delete risk.

C. Highlight Hack Tools – if Override actions configured for Security Risks is checked, for First action: select Quarantine risk or Delete risk.

D. Highlight Joke Programs – if Override actions configured for Security Risks is checked, for First action: select Quarantine risk or Delete risk.

E. Highlight Other – if Override actions configured for Security Risks is checked, for First action: select Quarantine risk or Delete risk.

F. Highlight Remote Access – if Override actions configured for Security Risks is checked, for First action: select Quarantine risk or Delete risk.

G. Highlight Spyware – if Override actions configured for Security Risks is checked, for First action: select Quarantine risk or Delete risk.

H. Highlight Trackware - if Override actions configured for Security Risks is checked, for First action: select Quarantine risk or Delete risk.

Group ID (Vulid): V-14607
Group Title: DTAS086-Symantec Antivirus autoprotect email secon
Rule ID: SV-23693r1_rule
Severity: CAT II
Rule Version (STIG-ID): DTAS086
Rule Title: The Symantec Antivirus Auto-Protect parameter for Email Security Risks Second Action is incorrect.

Vulnerability Discussion: This setting is required for the Auto-Protect email Security Risks second ("If first action fails") action policy. When a Security Risk such as Adware or Dialers is detected, the second action to be performed must be the option to delete risk, or quarantine the risk.

Responsibility: System Administrator

Check Content:
Procedure: This is a multiple step process to ensure compliance. Non-compliance points are identified throughout the procedures.
Note: This check is for email clients. Substitute your email application name (InternetMail, LotusNotes, or MicrosoftExchangeClient) into the registry string indicated by EmailName.
If email client is not installed, this check is NA.
Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\ INTEL\LANDesk\VirusProtect6\CurrentVersion\
Storages\EmailName \RealTimeScan\Expanded
Criteria: If the value of SecondAction is not 1 or 3, this is a finding.
If the value SecondAction is 1 or 3 then check each of the following steps. Each of the 8 parts (A-H) must be in compliance for the vulnerability to be considered not a finding.
A - If the value of OverrideDefaultActions within HKLM\Software\ INTEL\LANDesk\VirusProtect6 \CurrentVersion\Storages\EmailName \RealTimeScan\Expanded\TCID-10
If the value is 0 or the value is not there, this part is compliant.
If the value is 1, then check the SecondAction within HKLM\Software\ INTEL\LANDesk\VirusProtect6\CurrentVersion\Storages\EmailName \RealTimeScan\Expanded\TCID-10
If the value is 1 or 3, this is compliant, otherwise this is a finding.
B - If the value of OverrideDefaultActions within HKLM\Software\ INTEL\LANDesk\VirusProtect6 \CurrentVersion\Storages\EmailName \RealTimeScan\Expanded\TCID-11
If the value is 0 or the value is not there, this part is compliant.
If the value is 1, then check the SecondAction within HKLM\Software\ INTEL\LANDesk\VirusProtect6\CurrentVersion\Storages\EmailName \RealTimeScan\Expanded\TCID-11
If the value is 1 or 3, this is compliant, otherwise this is a finding.
C - If the value of OverrideDefaultActions within HKLM\Software\ INTEL\LANDesk\VirusProtect6 \CurrentVersion\Storages\EmailName \RealTimeScan\Expanded\TCID-4
If the value is 0 or the value is not there, this part is compliant.
If the value is 1, then check the SecondAction within HKLM\Software\ INTEL\LANDesk\VirusProtect6\CurrentVersion\Storages\EmailName \RealTimeScan\Expanded\TCID-4
If the value is 1 or 3, this is compliant, otherwise this is a finding.
D - If the value of OverrideDefaultActions within HKLM\Software\ INTEL\LANDesk\VirusProtect6 \CurrentVersion\Storages\EmailName \RealTimeScan\Expanded\TCID-5
If the value is 0 or the value is not there, this part is compliant.
If the value is 1, then check the SecondAction within HKLM\Software\ INTEL\LANDesk\VirusProtect6\CurrentVersion\Storages\EmailName \RealTimeScan\Expanded\TCID-5
If the value is 1 or 3, this is compliant, otherwise this is a finding.
E - If the value of OverrideDefaultActions within HKLM\Software\ INTEL\LANDesk\VirusProtect6 \CurrentVersion\Storages\EmailName \RealTimeScan\Expanded\TCID-6
If the value is 0 or the value is not there, this part is compliant.
If the value is 1, then check the SecondAction within HKLM\Software\ INTEL\LANDesk\VirusProtect6\CurrentVersion\Storages\EmailName \RealTimeScan\Expanded\TCID-6
If the value is 1 or 3, this is compliant, otherwise this is a finding.
F - If the value of OverrideDefaultActions within HKLM\Software\ INTEL\LANDesk\VirusProtect6 \CurrentVersion\Storages\EmailName \RealTimeScan\Expanded\TCID-7
If the value is 0 or the value is not there, this part is compliant.
If the value is 1, then check the SecondAction within HKLM\Software\ INTEL\LANDesk\VirusProtect6\CurrentVersion\Storages\EmailName \RealTimeScan\Expanded\TCID-7
If the value is 1 or 3, this is compliant, otherwise this is a finding.

G - If the value of OverrideDefaultActions within HKLM\Software\ INTEL\LANDesk\VirusProtect6 \CurrentVersion\Storages\EmailName \RealTimeScan\Expanded\TCID-8
If the value is 0 or the value is not there, this part is compliant.
If the value is 1, then check the SecondAction within HKLM\Software\ INTEL\LANDesk\VirusProtect6\CurrentVersion\Storages\EmailName \RealTimeScan\Expanded\TCID-8
If the value is 1 or 3, this is compliant, otherwise this is a finding.
H - If the value of OverrideDefaultActions within HKLM\Software\ INTEL\LANDesk\VirusProtect6 \CurrentVersion\Storages\EmailName \RealTimeScan\Expanded\TCID-9
If the value is 0 or the value is not there, this part is compliant.
If the value is 1, then check the SecondAction within HKLM\Software\ INTEL\LANDesk\VirusProtect6\CurrentVersion\Storages\EmailName \RealTimeScan\Expanded\TCID-9
If the value is 1 or 3, this is compliant, otherwise this is a finding.

Check Content:
Procedure: This is a multiple step process. Non-compliance points are identified throughout the procedures.

From the Symantec Enterprise Server, Symantec System Center Console: select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Client Auto-Protect Options -> email name tab (where “email name” is the email client type; options are Internet E-mail, Lotus Notes, and Microsoft Exchange) -> Actions -> highlight Security Risks: observe option for If first action fails:

Criteria: If the option selected for Security Risks If first action fails is not “Quarantine risk” or “Delete risk”, this is a finding.

If the selection for If first action fails is “Quarantine risk” or “Delete risk”, continue with each of the following steps. Each of the 8 parts (A – H) must be in compliance for the vulnerability to be considered not a finding.

A. Highlight Adware

If Override actions configured for Security Risks is not checked, this part is compliant.

If Override actions configured for Security Risks is checked: for If first action fails if Quarantine risk or Delete risk are selected, this is compliant, otherwise this is a finding.

B. Highlight Dialers

If Override actions configured for Security Risks is not checked, this part is compliant.

If Override actions configured for Security Risks is checked: for If first action fails if Quarantine risk or Delete risk are selected, this is compliant, otherwise this is a finding.

C. Highlight Hack Tools

If Override actions configured for Security Risks is not checked, this part is compliant.

If Override actions configured for Security Risks is checked: for If first action fails if Quarantine risk or Delete risk are selected, this is compliant, otherwise this is a finding.

D. Highlight Joke Programs

If Override actions configured for Security Risks is not checked, this part is compliant.

If Override actions configured for Security Risks is checked: for If first action fails if Quarantine risk or Delete risk are selected, this is compliant, otherwise this is a finding.

E. Highlight Other

If Override actions configured for Security Risks is not checked, this part is compliant.

If Override actions configured for Security Risks is checked: for If first action fails if Quarantine risk or Delete risk are selected, this is compliant, otherwise this is a finding.

F. Highlight Remote Access

If Override actions configured for Security Risks is not checked, this part is compliant.

If Override actions configured for Security Risks is checked: for If first action fails if Quarantine risk or Delete risk are selected, this is compliant, otherwise this is a finding.

G. Highlight Spyware

If Override actions configured for Security Risks is not checked, this part is compliant.

If Override actions configured for Security Risks is checked: for If first action fails if Quarantine risk or Delete risk are selected, this is compliant, otherwise this is a finding.

H. Highlight Trackware

If Override actions configured for Security Risks is not checked, this part is compliant.

If Override actions configured for Security Risks is checked: for If first action fails if Quarantine risk or Delete risk are selected, this is compliant, otherwise this is a finding.

Fix Text: From the Symantec Enterprise Server, Symantec System Center Console: select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Client Auto-Protect Options -> email name tab (where “email name” is the email client type; options are Internet E-mail, Lotus Notes, and Microsoft Exchange) -> Actions -> Highlight Security Risks: under the Actions tab If first action fails: select one of the following “Quarantine risk” or “Delete risk”.

If the selection for First action is “Quarantine risk” or “Delete risk”, continue with each of the following steps. Each of the 8 parts (A – H) must be in compliance for the vulnerability to be considered not a finding.

A. Highlight Adware - if Override actions configured for Security Risks is checked, for If first action fails: select Quarantine risk or Delete risk.

B. Highlight Dialers - if Override actions configured for Security Risks is checked, for If first action fails: select Quarantine risk or Delete risk.

C. Highlight Hack Tools – if Override actions configured for Security Risks is checked, for If first action fails: select Quarantine risk or Delete risk.

D. Highlight Joke Programs – if Override actions configured for Security Risks is checked, for If first action fails: select Quarantine risk or Delete risk.

E. Highlight Other – if Override actions configured for Security Risks is checked, for If first action fails: select Quarantine risk or Delete risk.

F. Highlight Remote Access – if Override actions configured for Security Risks is checked, for If first action fails: select Quarantine risk or Delete risk.

G. Highlight Spyware – if Override actions configured for Security Risks is checked, for If first action fails: select Quarantine risk or Delete risk.

H. Highlight Trackware - if Override actions configured for Security Risks is checked, for If first action fails: select Quarantine risk or Delete risk.

Group ID (Vulid): V-14609
Group Title: DTAS091-Symantec Antivirus weekly scan load points
Rule ID: SV-23694r1_rule
Severity: CAT II
Rule Version (STIG-ID): DTAS091
Rule Title: The Symantec Antivirus weekly scan parameter for scanning load points is incorrect.

Vulnerability Discussion: This setting is required to configure the scanning of load points. "Load points" are defined by Symantec AV as "Common Infection locations".

Responsibility: System Administrator

Check Content:
From the Symantec Enterprise Server- Symantec System Center Console - select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Scheduled Scans -> Highlight the client server weekly scan -> select Edit -> select Scan Settings -> Observe that “Common infection locations (load points)” is selected.

Criteria: If the option “Common infection locations (load points)” is selected, this not a finding.

To evaluate this check from a client machine, navigate to the registry key:
HKLM\Software\Intel\Landesk\VirusProtect6\CurrentVersion\LocalScans\ClientServerScheduledScan_1.
Note: In the key ClientServerScheduledScan_1, the 1 indicates the entry number for the scan. It may be necessary to review all ClientServerScheduledScan_X keys in the LocalScans branch to evaluate this check.

Criteria: If the value of ScanLoadPoints is 1, this not a finding.

Fix Text: From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On-Access General Policies. Select from the Policy column the policy associated with the On-Access General Policies. Under the Blocking tab, locate the "Block the connection:" label. Select the "Block the connection when a threatened file is detected in a shared folder" option.

Group ID (Vulid): V-14610
Group Title: DTAS092-Symantec Antivirus weekly scan well knowns
Rule ID: SV-23695r1_rule
Severity: CAT II
Rule Version (STIG-ID): DTAS092
Rule Title: The Symantec Antivirus weekly scan parameter for well knowns before others is incorrect.

Vulnerability Discussion: This setting is required to configure scanning locations of well-known vuruses and security risks.

Responsibility: System Administrator

Check Content:
From the Symantec Enterprise Server- Symantec System Center Console - select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Scheduled Scans -> Highlight the client server weekly scan -> select Edit -> select Scan Settings ->Observe that “Locations of well known viruses and security risks” is selected.

Criteria: If the option “Locations of well known viruses and security risks” is selected, this not a finding.

To evaluate this check on the client machine, navigate to the following registry key:
HKLM\Software\Intel\Landesk\VirusProtect6\CurrentVersion\LocalScans\ClientServerScheduledScan_1.
Note: In the key ClientServerScheduledScan_1, the 1 indicates the entry number for the scan. It may be necessary to review all ClientServerScheduledScan_X keys in the LocalScans branch to evaluate this check.

Criteria: If the value of ScanERASERDEFS is 1, this is not a finding.

Fix Text: From the Symantec Enterprise Server- Symantec System Center Console - select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Scheduled Scans -> Highlight the client server weekly scan -> select Edit -> select Scan Settings -> select “Locations of well known viruses and security risks”.

Group ID (Vulid): V-14611
Group Title: DTAS093-Symantec Antivirus weekly scan macro first
Rule ID: SV-23701r1_rule
Severity: CAT II
Rule Version (STIG-ID): DTAS093
Rule Title: The Symantec Antivirus weekly scan parameter for macro virus first action is incorrect.

Vulnerability Discussion: This setting is required for the weekly scan Macro virus First action policy. When a Macro virus is detected, the first action to be performed must be the option to delete risk, clean risk, or quarantine the risk.

Responsibility: System Administrator

Check Content:
From the Symantec Enterprise Server- Symantec System Center Console - select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Scheduled Scans -> Highlight the client server weekly scan -> select Edit -> select Scan Settings -> Actions -> Highlight Macro virus -> Ensure for First action: Clean risk, Quarantine risk, or Delete risk is selected.

Criteria: If the options selected for Macro virus First action are Clean risk, Quarantine risk, or Delete risk, this is not a finding.

To evaluate this check on the client machine, navigate to the following registry key:
HKLM\Software\Intel\Landesk\VirusProtect6\CurrentVersion\LocalScans\ClientServerScheduledScan_1.
Note: In the key ClientServerScheduledScan_1, the 1 indicates the entry number for the scan. It may be necessary to review all ClientServerScheduledScan_X keys in the LocalScans branch to evaluate this check.

Criteria: If the value of FirstMacroAction is 1, 3, or 5, this is not a finding.

Fix Text: From the Symantec Enterprise Server- Symantec System Center Console - select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Scheduled Scans -> Highlight the client server weekly scan -> select Edit -> select Scan Setings -> Actions -> Highlight Macro virus: First action:, select "Clean risk, Quarantine risk, or Delete risk".

Group ID (Vulid): V-14612
Group Title: DTAS094-Symantec Antivirus weekly scan macro secon
Rule ID: SV-23696r1_rule
Severity: CAT II
Rule Version (STIG-ID): DTAS094
Rule Title: The Symantec Antivirus weekly scan parameter for macro virus second action is incorrect.

Vulnerability Discussion: This setting is required for the weekly scan parameter Macro virus Second action policy. When a non-Macro virus is detected, the Second action ("If first action fails") to be performed must be the option to delete risk, clean risk, or quarantine the risk.

Responsibility: System Administrator

Check Content:
From the Symantec Enterprise Server- Symantec System Center Console - select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Scheduled Scans -> Highlight the client server weekly scan -> select Edit -> select Scan Settings -> Actions -> Highlight Macro virus: Ensure for If first action fails: Clean risk, Quarantine risk, or Delete risk is selected.

Criteria: If the options selected for Macro virus If first action fails are Clean risk, Quarantine risk, or Delete risk, this is not a finding.

To evaluate this check on the client machine, navigate to the following registry key:
HKLM\Software\Intel\Landesk\VirusProtect6\CurrentVersion\LocalScans\ClientServerScheduledScan_1.
Note: in the key ClientServerScheduledScan_1, the 1 indicates the entry number for the scan. It may be necessary to review all ClientServerScheduledScan_X keys in the LocalScans branch to evaluate this check.

Criteria: If the value of SeconMacroAction is 1, 3, or 5, this is not a finding.

Fix Text: From the Symantec Enterprise Server- Symantec System Center Console - select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Scheduled Scans -> Highlight the client server weekly scan -> select Edit -> select Scan Settings -> Actions -> Highlight Macro virus: If first action fails:, select "Clean risk, Quarantine risk, or Delete risk".

Group ID (Vulid): V-14613
Group Title: DTAS095-Symantec Antivirus weekly scan nonmacro fi
Rule ID: SV-23697r1_rule
Severity: CAT II
Rule Version (STIG-ID): DTAS095
Rule Title: The Symantec Antivirus weekly scan parameter for non-macro first action virus is incorrect.

Vulnerability Discussion: This setting is required for the weekly scan parameter non-Macro virus First action policy. When a non-Macro virus is detected, the first action to be performed must be the option to delete risk, clean risk, or quarantine the risk.

Responsibility: System Administrator

Check Content:
From the Symantec Enterprise Server- Symantec System Center Console - select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Scheduled Scans -> Highlight the client server weekly scan -> select Edit -> select Scan Settings -> Actions -> Highlight Non-Macro Virus: Ensure for First Action: Clean risk, Quarantine risk, or Delete risk is selected.

Criteria: If the options selected for Non-Macro virus First action are Clean risk, Quarantine risk, or Delete risk, this is not a finding.

To evaluate this check on the client machine, navigate to the following registry key:
HKLM\Software\Intel\Landesk\VirusProtect6\CurrentVersion\LocalScans\ClientServerScheduledScan_1.
Note: In the key ClientServerScheduledScan_1, the 1 indicates the entry number for the scan. It may be necessary to review all ClientServerScheduledScan_X keys in the LocalScans branch to evaluate this check.

Criteria: If the value of FirstAction is 1, 3, or 5, this is not a finding.

Fix Text: From the Symantec Enterprise Server- Symantec System Center Console - select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Scheduled Scans -> Highlight the client server weekly scan -> select Edit -> select Scan Settings -> Actions -> Highlight Non-Macro Virus: First Action:, select "Clean risk, Quarantine risk, or Delete risk".

Group ID (Vulid): V-14615
Group Title: DTAS096-Symantec Antivirus autoprotect nonmacro se
Rule ID: SV-23698r1_rule
Severity: CAT II
Rule Version (STIG-ID): DTAS096
Rule Title: The Symantec Antivirus Auto-Protect parameter for check non-macro second action is incorrect.

Vulnerability Discussion: This setting is required for the Auto-Protect parameter non-Macro virus second action policy. When an email Macro virus is detected, the second action ("If first action fails:") to be performed must be the option to delete risk, clean risk, or quarantine the risk.

Responsibility: System Administrator

Check Content:
From the Symantec Enterprise Server- Symantec System Center Console - select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Scheduled Scans -> Highlight the client server weekly scan -> select Edit -> select Scan Settings -> Actions -> Highlight Non-macro virus: Ensure for If first action fails: Clean risk, Quarantine risk, or Delete risk is selected.

Criteria: If the options selected for Non-Macro virus If first action fails are Clean risk, Quarantine risk, or Delete risk, this is not a finding.

To evaluate this check on the client machine, navigate to the following registry key:
HKLM\Software\Intel\Landesk\VirusProtect6\CurrentVersion\LocalScans\ClientServerScheduledScan_1.
Note: In the key ClientServerScheduledScan_1, the 1 indicates the entry number for the scan. It may be necessary to review all ClientServerScheduledScan_X keys in the LocalScans branch to evaluate this check.

Criteria: If the value of SecondAction is 1, 3, or 5, this is not a finding.

Fix Text: From the Symantec Enterprise Server- Symantec System Center Console - select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Scheduled Scans -> Highlight the client server weekly scan -> select Edit -> select Scan Settings -> Actions -> Highlight Non-macro virus: If first action fails:, select "Clean risk, Quarantine risk, or Delete risk".

Group ID (Vulid): V-14616
Group Title: DTAS097-Symantec Antivirus weekly scan risk first
Rule ID: SV-23699r1_rule
Severity: CAT II
Rule Version (STIG-ID): DTAS097
Rule Title: The Symantec Antivirus weekly scan parameter for Security Risks first action is incorrect.

Vulnerability Discussion: This setting is required for the weekly scan parameter Security Risks First action policy. When a Security Risk is detected, the first action to be performed must be the option to delete risk, clean risk, or quarantine the risk.

Responsibility: System Administrator

Check Content:
Procedure: This is a multiple step process. Non-compliance points are identified throughout the procedures.

From the Symantec Enterprise Server- Symantec System Center Console - select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Scheduled Scans -> Highlight the client server weekly scan -> select Edit -> select Scan Settings -> Actions -> highlight Security Risks: observe option for First action.

Criteria: If the option selected for Security Risks First action is not “Quarantine risk” or “Delete risk”, this is a finding.

If the selection for First action is “Quarantine risk” or “Delete risk”, continue with each of the following steps. Each of the 8 parts (A – H) must be in compliance for the vulnerability to be considered not a finding.

A. Highlight Adware

If Override actions configured for Security Risks is not checked, this part is compliant.

If Override actions configured for Security Risks is checked: for First action if Quarantine risk or Delete risk are selected, this is compliant, otherwise this is a finding.

B. Highlight Dialers

If Override actions configured for Security Risks is not checked, this part is compliant.

If Override actions configured for Security Risks is checked: for First action if Quarantine risk or Delete risk are selected, this is compliant, otherwise this is a finding.

C. Highlight Hack Tools

If Override actions configured for Security Risks is not checked, this part is compliant.

If Override actions configured for Security Risks is checked: for First action if Quarantine risk or Delete risk are selected, this is compliant, otherwise this is a finding.

D. Highlight Joke Programs

If Override actions configured for Security Risks is not checked, this part is compliant.

If Override actions configured for Security Risks is checked: for First action if Quarantine risk or Delete risk are selected, this is compliant, otherwise this is a finding.

E. Highlight Other

If Override actions configured for Security Risks is not checked, this part is compliant.

If Override actions configured for Security Risks is checked: for First action if Quarantine risk or Delete risk are selected, this is compliant, otherwise this is a finding.

F. Highlight Remote Access

If Override actions configured for Security Risks is not checked, this part is compliant.

If Override actions configured for Security Risks is checked: for First action if Quarantine risk or Delete risk are selected, this is compliant, otherwise this is a finding.

G. Highlight Spyware

If Override actions configured for Security Risks is not checked, this part is compliant.

If Override actions configured for Security Risks is checked: for First action if Quarantine risk or Delete risk are selected, this is compliant, otherwise this is a finding.

H. Highlight Trackware

If Override actions configured for Security Risks is not checked, this part is compliant.

If Override actions configured for Security Risks is checked: for First action if Quarantine risk or Delete risk are selected, this is compliant, otherwise this is a finding.

To evaluate this check on the client machine, perform the following procedures. This is a multiple step process to ensure compliance. Non-compliance points are
identified throughout the procedures. Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Intel\Landesk\VirusProtect6\CurrentVersion\LocalScans\ClientServerScheduledScan_1
\Expanded.
Note: In the key ClientServerScheduledScan_1, the 1 indicates the entry number for the scan. It may be necessary to review all ClientServerScheduledScan_X keys in the LocalScans branch to evaluate this check.

Criteria: If the value of FirstAction is not 1 or 3, this is a finding.

If the value FirstAction is 1 or 3, then check each of the following steps. Each of the 8 parts (A-H)
must be in compliance for the vulnerability to be considered not a finding.

A - If the value of OverrideDefaultActions within HKLM\Software\Intel\Landesk\VirusProtect6
\CurrentVersion\LocalScans\ClientServerScheduledScan_1\Expanded\TCID-10
If the value is 0 or the value is not there, this part is compliant.
If the value is 1, then check the FirstAction within HKLM\Software\Intel\Landesk\VirusProtect6
\CurrentVersion\LocalScans\ClientServerScheduledScan_1\Expanded\TCID-10
If the value is 1 or 3, this is compliant, otherwise this is a finding.
B - If the value of OverrideDefaultActions within HKLM\Software\Intel\Landesk\VirusProtect6
\CurrentVersion\LocalScans\ClientServerScheduledScan_1\Expanded\TCID-11
If the value is 0 or the value is not there, this part is compliant.
If the value is 1, then check the FirstAction within HKLM\Software\Intel\Landesk\VirusProtect6
\CurrentVersion\LocalScans\ClientServerScheduledScan_1\Expanded\TCID-11
If the value is 1 or 3, this is compliant, otherwise this is a finding.
C - If the value of OverrideDefaultActions within HKLM\Software\Intel\Landesk\VirusProtect6
\CurrentVersion\LocalScans\ClientServerScheduledScan_1\Expanded\TCID-4
If the value is 0 or the value is not there, this part is compliant.
If the value is 1, then check the FirstAction within HKLM\Software\Intel\Landesk\VirusProtect6
\CurrentVersion\LocalScans\ClientServerScheduledScan_1\Expanded\TCID-4
If the value is 1 or 3, this is compliant, otherwise this is a finding.
D - If the value of OverrideDefaultActions within HKLM\Software\Intel\Landesk\VirusProtect6

\CurrentVersion\LocalScans\ClientServerScheduledScan_1\Expanded\TCID-5
If the value is 0 or the value is not there, this part is compliant.
If the value is 1, then check the FirstAction within HKLM\Software\Intel\Landesk\VirusProtect6
\CurrentVersion\LocalScans\ClientServerScheduledScan_1\Expanded\TCID-5
If the value is 1 or 3, this is compliant, otherwise this is a finding.
E - If the value of OverrideDefaultActions within HKLM\Software\Intel\Landesk\VirusProtect6
\CurrentVersion\LocalScans\ClientServerScheduledScan_1\Expanded\TCID-6
If the value is 0 or the value is not there, this part is compliant.
If the value is 1, then check the FirstAction within HKLM\Software\Intel\Landesk\VirusProtect6
\CurrentVersion\LocalScans\ClientServerScheduledScan_1\Expanded\TCID-6
If the value is 1 or 3, this is compliant, otherwise this is a finding.
F - If the value of OverrideDefaultActions within HKLM\Software\Intel\Landesk\VirusProtect6
\CurrentVersion\LocalScans\ClientServerScheduledScan_1\Expanded\TCID-7
If the value is 0 or the value is not there, this part is compliant.
If the value is 1, then check the FirstAction within HKLM\Software\Intel\Landesk\VirusProtect6
\CurrentVersion\LocalScans\ClientServerScheduledScan_1\Expanded\TCID-7
If the value is 1 or 3, this is compliant, otherwise this is a finding.
G - If the value of OverrideDefaultActions within HKLM\Software\Intel\Landesk\VirusProtect6
\CurrentVersion\LocalScans\ClientServerScheduledScan_1\Expanded\TCID-8
If the value is 0 or the value is not there, this part is compliant.
If the value is 1, then check the FirstAction within HKLM\Software\Intel\Landesk\VirusProtect6
\CurrentVersion\LocalScans\ClientServerScheduledScan_1\Expanded\TCID-8
If the value is 1 or 3, this is compliant, otherwise this is a finding.
H - If the value of OverrideDefaultActions within HKLM\Software\Intel\Landesk\VirusProtect6
\CurrentVersion\LocalScans\ClientServerScheduledScan_1\Expanded\TCID-9
If the value is 0 or the value is not there, this part is compliant.
If the value is 1, then check the FirstAction within HKLM\Software\Intel\Landesk\VirusProtect6
\CurrentVersion\LocalScans\ClientServerScheduledScan_1\Expanded\TCID-9
If the value is 1 or 3, this is compliant, otherwise this is a finding.

Fix Text: From the Symantec Enterprise Server- Symantec System Center Console - select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Scheduled Scans -> Highlight the client server weekly scan -> select Edit -> select Scan Settings -> Actions -> Highlight Security Risks: under the Actions tab First action: select one of the following “Quarantine risk” or “Delete risk”.

If the selection for First action is “Quarantine risk” or “Delete risk”, continue with each of the following steps. Each of the 8 parts (A – H) must be in compliance for the vulnerability to be considered not a finding.

A. Highlight Adware - if Override actions configured for Security Risks is checked, for First action: select Quarantine risk or Delete risk.

B. Highlight Dialers - if Override actions configured for Security Risks is checked, for First action: select Quarantine risk or Delete risk.

C. Highlight Hack Tools – if Override actions configured for Security Risks is checked, for First action: select Quarantine risk or Delete risk.

D. Highlight Joke Programs – if Override actions configured for Security Risks is checked, for First action: select Quarantine risk or Delete risk.

E. Highlight Other – if Override actions configured for Security Risks is checked, for First action: select Quarantine risk or Delete risk.

F. Highlight Remote Access – if Override actions configured for Security Risks is checked, for First action: select Quarantine risk or Delete risk.

G. Highlight Spyware – if Override actions configured for Security Risks is checked, for First action: select Quarantine risk or Delete risk.

H. Highlight Trackware - if Override actions configured for Security Risks is checked, for First action: select Quarantine risk or Delete risk.

Group ID (Vulid): V-14617
Group Title: DTAS098-The Symantec Antivirus weekly scan paramet
Rule ID: SV-23700r1_rule
Severity: CAT II
Rule Version (STIG-ID): DTAS098
Rule Title: The Symantec Antivirus weekly scan parameter for Security Risks second action is incorrect.

Vulnerability Discussion: This setting is required for the weekly scan parameter Security Risks second ("If first action fails") action policy. When a Security Risk, such as Adware or Dialers, is detected, the second action to be performed must be the option to delete risk, or quarantine the risk.

Responsibility: System Administrator

Check Content:
Procedure: This is a multiple step process. Non-compliance points are identified throughout the procedures.

From the Symantec Enterprise Server- Symantec System Center Console - select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Scheduled Scans -> Highlight the client server weekly scan -> select Edit -> select Scan Settings -> Actions -> highlight Security Risks: observe option for If first action fails.

Criteria: If the option selected for Security Risks If first action fails is not “Quarantine risk” or “Delete risk”, this is a finding.

If the selection for If first action fails is “Quarantine risk” or “Delete risk”, continue with each of the following steps. Each of the 8 parts (A – H) must be in compliance for the vulnerability to be considered not a finding.

A. Highlight Adware

If Override actions configured for Security Risks is not checked, this part is compliant.

If Override actions configured for Security Risks is checked: for If first action fails if Quarantine risk or Delete risk are selected, this is compliant, otherwise this is a finding.

B. Highlight Dialers

If Override actions configured for Security Risks is not checked, this part is compliant.

If Override actions configured for Security Risks is checked: for If first action fails if Quarantine risk or Delete risk are selected, this is compliant, otherwise this is a finding.

C. Highlight Hack Tools

If Override actions configured for Security Risks is not checked, this part is compliant.

If Override actions configured for Security Risks is checked: for If first action fails if Quarantine risk or Delete risk are selected, this is compliant, otherwise this is a finding.

D. Highlight Joke Programs

If Override actions configured for Security Risks is not checked, this part is compliant.

If Override actions configured for Security Risks is checked: for If first action fails if Quarantine risk or Delete risk are selected, this is compliant, otherwise this is a finding.

E. Highlight Other

If Override actions configured for Security Risks is not checked, this part is compliant.

If Override actions configured for Security Risks is checked: for If first action fails if Quarantine risk or Delete risk are selected, this is compliant, otherwise this is a finding.

F. Highlight Remote Access

If Override actions configured for Security Risks is not checked, this part is compliant.

If Override actions configured for Security Risks is checked: for If first action fails if Quarantine risk or Delete risk are selected, this is compliant, otherwise this is a finding.

G. Highlight Spyware

If Override actions configured for Security Risks is not checked, this part is compliant.

If Override actions configured for Security Risks is checked: for If first action fails if Quarantine risk or Delete risk are selected, this is compliant, otherwise this is a finding.

H. Highlight Trackware

If Override actions configured for Security Risks is not checked, this part is compliant.

If Override actions configured for Security Risks is checked: for If first action fails if Quarantine risk or Delete risk are selected, this is compliant, otherwise this is a finding.

To evaluate this check on the client machine, perform the following procedures. This is a multiple step process to ensure compliance. Non-compliance points are
identified throughout the procedures. Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Intel\Landesk\VirusProtect6\CurrentVersion\LocalScans\ClientServerScheduledScan_1
\Expanded.
Note: In the key ClientServerScheduledScan_1, the 1 indicates the entry number for the scan. It may be necessary to review all ClientServerScheduledScan_X keys in the LocalScans branch to evaluate this check.

Criteria: If the value of SecondAction is not 1 or 3, this is a finding.

If the value SecondAction is 1 or 3, then check each of the following steps. Each of the 8 parts (A-H) must be in compliance for the vulnerability to be considered not a finding.

A - If the value of OverrideDefaultActions within HKLM\Software\Intel\Landesk\VirusProtect6
\CurrentVersion\LocalScans\ClientServerScheduledScan_1\Expanded\TCID-10
If the value is 0 or the value is not there, this part is compliant.
If the value is 1, then check the SecondAction within HKLM\Software\Intel\Landesk\VirusProtect6
\CurrentVersion\LocalScans\ClientServerScheduledScan_1\Expanded\TCID-10
If the value is 1 or 3, this is compliant, otherwise this is a finding.
B - If the value of OverrideDefaultActions within HKLM\Software\Intel\Landesk\VirusProtect6
\CurrentVersion\LocalScans\ClientServerScheduledScan_1\Expanded\TCID-11

If the value is 0 or the value is not there, this part is compliant.
If the value is 1, then check the SecondAction within HKLM\Software\Intel\Landesk\VirusProtect6
\CurrentVersion\LocalScans\ClientServerScheduledScan_1\Expanded\TCID-11
If the value is 1 or 3, this is compliant, otherwise this is a finding.
C - If the value of OverrideDefaultActions within HKLM\Software\Intel\Landesk\VirusProtect6
\CurrentVersion\LocalScans\ClientServerScheduledScan_1\Expanded\TCID-4
If the value is 0 or the value is not there, this part is compliant.
If the value is 1, then check the SecondAction within HKLM\Software\Intel\Landesk\VirusProtect6
\CurrentVersion\LocalScans\ClientServerScheduledScan_1\Expanded\TCID-4
If the value is 1 or 3, this is compliant, otherwise this is a finding.
D - If the value of OverrideDefaultActions within HKLM\Software\Intel\Landesk\VirusProtect6
\CurrentVersion\LocalScans\ClientServerScheduledScan_1\Expanded\TCID-5
If the value is 0 or the value is not there, this part is compliant.
If the value is 1, then check the SecondAction within HKLM\Software\Intel\Landesk\VirusProtect6
\CurrentVersion\LocalScans\ClientServerScheduledScan_1\Expanded\TCID-5
If the value is 1 or 3, this is compliant, otherwise this is a finding.
E - If the value of OverrideDefaultActions within HKLM\Software\Intel\Landesk\VirusProtect6
\CurrentVersion\LocalScans\ClientServerScheduledScan_1\Expanded\TCID-6
If the value is 0 or the value is not there, this part is compliant.
If the value is 1, then check the SecondAction within HKLM\Software\Intel\Landesk\VirusProtect6
\CurrentVersion\LocalScans\ClientServerScheduledScan_1\Expanded\TCID-6
If the value is 1 or 3, this is compliant, otherwise this is a finding.
F - If the value of OverrideDefaultActions within HKLM\Software\Intel\Landesk\VirusProtect6
\CurrentVersion\LocalScans\ClientServerScheduledScan_1\Expanded\TCID-7
If the value is 0 or the value is not there, this part is compliant.
If the value is 1, then check the SecondAction within HKLM\Software\Intel\Landesk\VirusProtect6
\CurrentVersion\LocalScans\ClientServerScheduledScan_1\Expanded\TCID-7
If the value is 1 or 3, this is compliant, otherwise this is a finding.
G - If the value of OverrideDefaultActions within HKLM\Software\Intel\Landesk\VirusProtect6
\CurrentVersion\LocalScans\ClientServerScheduledScan_1\Expanded\TCID-8
If the value is 0 or the value is not there, this part is compliant.
If the value is 1, then check the SecondAction within HKLM\Software\Intel\Landesk\VirusProtect6
\CurrentVersion\LocalScans\ClientServerScheduledScan_1\Expanded\TCID-8
If the value is 1 or 3, this is compliant, otherwise this is a finding.
H - If the value of OverrideDefaultActions within HKLM\Software\Intel\Landesk\VirusProtect6
\CurrentVersion\LocalScans\ClientServerScheduledScan_1\Expanded\TCID-9
If the value is 0 or the value is not there, this part is compliant.
If the value is 1, then check the SecondAction within HKLM\Software\Intel\Landesk\VirusProtect6
\CurrentVersion\LocalScans\ClientServerScheduledScan_1\Expanded\TCID-9
If the value is 1 or 3, this is compliant, otherwise this is a finding.

Fix Text: From the Symantec Enterprise Server- Symantec System Center Console - select System Hierarchy -> select [applicable "Server Group"] -> select [applicable "Client Group"] (right click) -> All Tasks -> Symantec Antivirus -> Scheduled Scans -> Highlight the client server weekly scan -> select Edit -> select Scan Settings -> Actions -> Highlight Security Risks: under the Actions tab If first action fails: select one of the following “Quarantine risk” or “Delete risk”.

If the selection for First action is “Quarantine risk” or “Delete risk”, continue with each of the following steps. Each of the 8 parts (A – H) must be in compliance for the vulnerability to be considered not a finding.

A. Highlight Adware - if Override actions configured for Security Risks is checked, for If first action fails: select Quarantine risk or Delete risk.

B. Highlight Dialers - if Override actions configured for Security Risks is checked, for If first action fails: select

Quarantine risk or Delete risk.

C. Highlight Hack Tools – if Override actions configured for Security Risks is checked, for If first action fails: select Quarantine risk or Delete risk.

D. Highlight Joke Programs – if Override actions configured for Security Risks is checked, for If first action fails: select Quarantine risk or Delete risk.

E. Highlight Other – if Override actions configured for Security Risks is checked, for If first action fails: select Quarantine risk or Delete risk.

F. Highlight Remote Access – if Override actions configured for Security Risks is checked, for If first action fails: select Quarantine risk or Delete risk.

G. Highlight Spyware – if Override actions configured for Security Risks is checked, for If first action fails: select Quarantine risk or Delete risk.

H. Highlight Trackware - if Override actions configured for Security Risks is checked, for If first action fails: select Quarantine risk or Delete risk.

Group ID (Vulid): V-19910
Group Title: Virus Signature Files older that 7 days.
Rule ID: SV-22091r1_rule
Severity: CAT I
Rule Version (STIG-ID): DTAG008
Rule Title: The antivirus signature file age exceeds 7 days.

Vulnerability Discussion: Antivirus signature files are updated almost daily by antivirus software vendors. These files are made available to antivirus clients as they are published. Keeping virus signature files as current as possible is vital to the security of any system.

Note: If the vendor or trusted site's files match the date of the signature files on the machine, this is not a finding.

Responsibility: System Administrator

Check Content:
On the client machine, locate Symantec AntiVirus icon in the system tray. Click icon to open Symantec AntiVirus configuration screen. Observe "Virus Definitions File" area.

Criteria: If the "Version:" date is older than 7 calendar days from the current date, this is a finding.

Note: If the vendor or trusted site's files are also older than 7 days and match the date of the signature files on the machine, this is not a finding.

Fix Text: Update client machines via the Symantec Enterprise Console. If this fails to update the client, update antivirus signature file as your local process describes (e.g. autoupdate or LiveUpdate).

UNCLASSIFIED